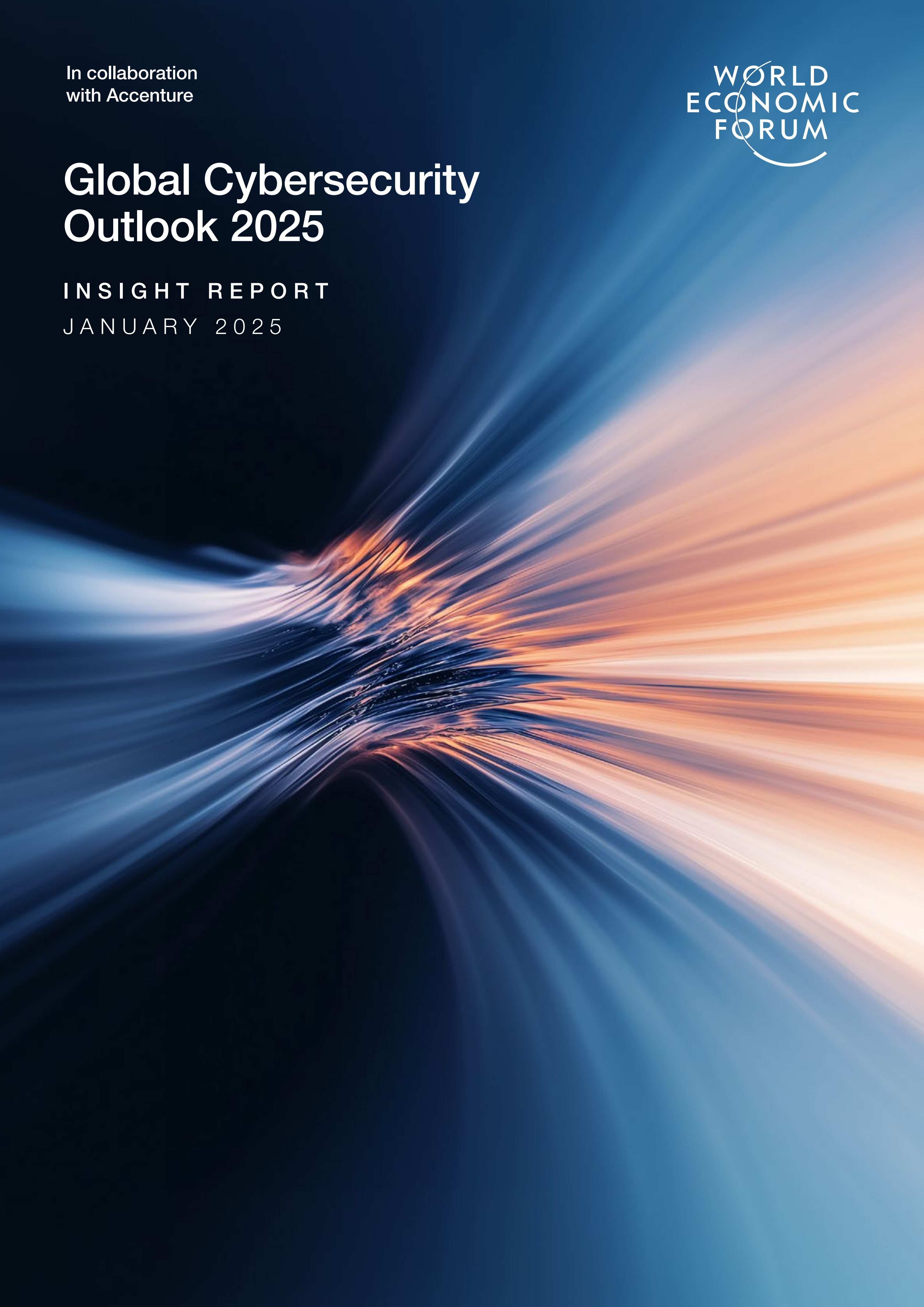
In collaboration
with Accenture

Global Cybersecurity Outlook 2025

INSIGHT REPORT

JANUARY 2025



Images: Getty Images

Contents

Disclaimer
This document is published by the World Economic Forum as a contribution to a project, insight area or interaction. The findings, interpretations and conclusions expressed herein are a result of a collaborative process facilitated and endorsed by the World Economic Forum but whose results do not necessarily represent the views of the World Economic Forum, nor the entirety of its Members, Partners or other stakeholders.

Foreword

Jeremy Jurgens
Managing Director,
World Economic Forum

Paolo Dal Cin
Global Security Lead,
Accenture

Following decades of relative stability, the world today is marked by increased geopolitical conflicts. The fallout of this turbulence in the digital realm – the growing prowess of cybercriminals, rapid advances in emerging technologies and widening cyber capabilities – have led to a cyberspace that is more complex than ever before. Against this backdrop, the *Global Cybersecurity Outlook* serves as an indispensable tool to help leaders navigate such complexity and identify essential actions to build resilient ecosystems.

Last year's report brought to the fore the prevailing inequity between the cyber haves and have-nots. Despite increased executive awareness of cybersecurity risks, the complexity in cyberspace is further exacerbating cyber inequity as resilient organizations pull ahead, while others struggle with limited resources. Amid increasingly interdependent supply chains, this cyber inequity is resulting in systemic points of failure with significant consequences for the overall resilience of the ecosystem.

The transformative potential of AI technologies presents both unprecedented risks and unmatched opportunities for cybersecurity. As organizations race to adopt AI, cybercriminals are moving at breakneck speed to exploit vulnerabilities while enhancing the efficacy of their methods. Cyber defenders, too, are leaving no stone unturned in harnessing the potential of these technologies to shift the balance in this growing AI arms race.

Looking to the future, the level of complexity shows no signs of abating. In a borderless cyberspace, greater collaboration between actors in the public and private sectors is crucial for safeguarding the benefits of digitalization for all. This is a call to action, and the time to act is now.

Executive summary

In a complex cyberspace characterized by geopolitical uncertainties, widening cyber inequity and sophisticated cyberthreats, leaders must adopt a security-first mindset.

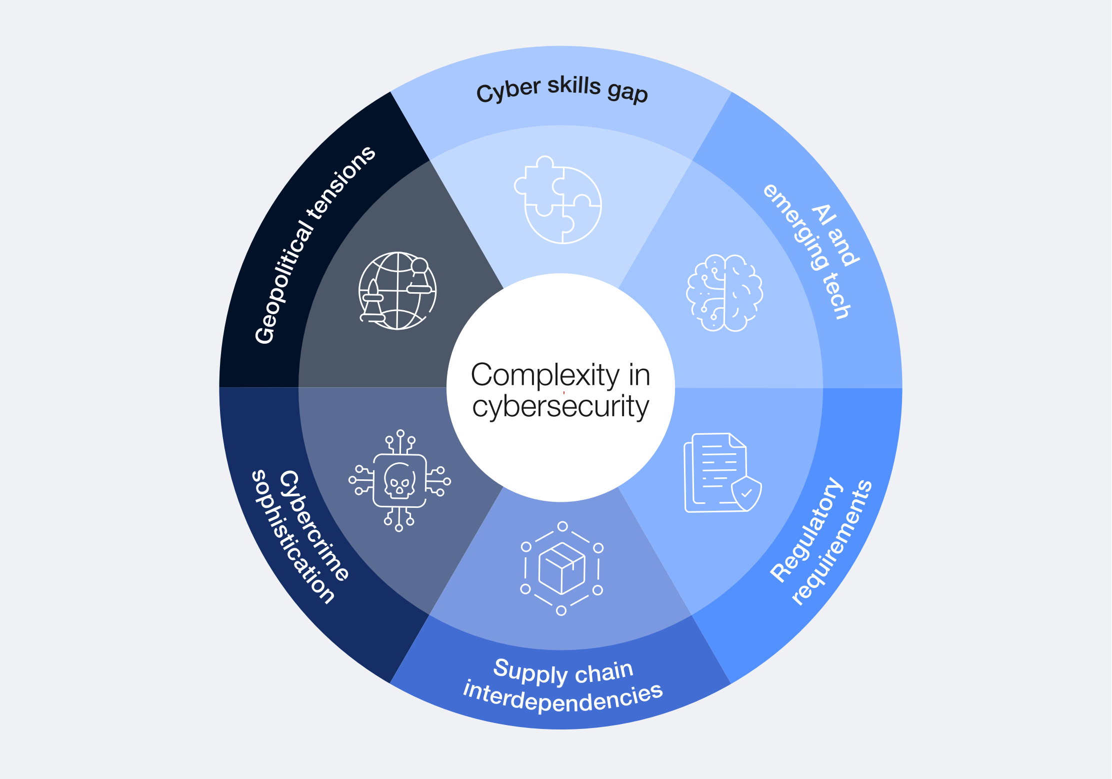
While the 2024 edition of the Global Cybersecurity Outlook highlighted the growing inequity in cyberspace, this year's report shines a light on the increasing complexity of the cyber landscape, which has profound and far-reaching implications for organizations and nations.

This complexity is driven by a series of compounding factors:

- Escalating geopolitical tensions are contributing to a more uncertain environment.
- Increased integration of and dependence on more complex supply chains is leading to a more opaque and unpredictable risk landscape.
- The rapid adoption of emerging technologies is contributing to new vulnerabilities as cybercriminals harness them effectively to achieve greater sophistication and scale.
- Simultaneously, the proliferation of regulatory requirements around the world is adding a significant compliance burden for organizations.

All of these challenges are exacerbated by a widening skills gap, making it extremely challenging to manage cyber risks effectively.

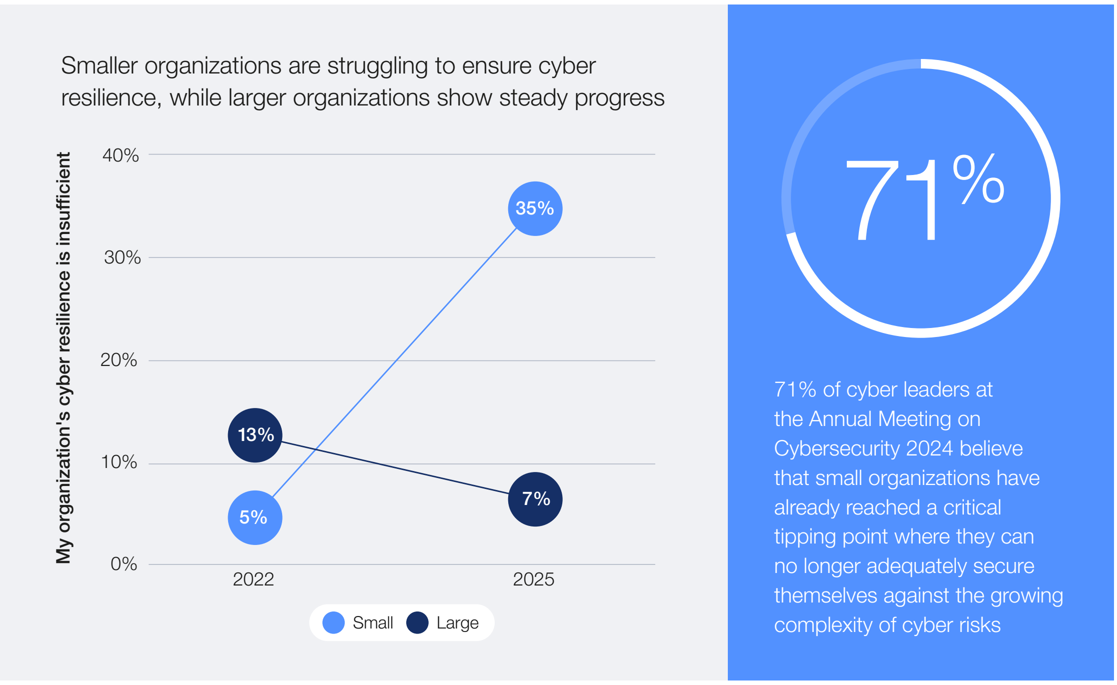
FIGURE A **Factors compounding the complex nature of cybersecurity**


Cyber skills gap
AI and emerging tech
Regulatory requirements
Supply chain interdependencies
Cybercrime sophistication
Geopolitical tensions
Complexity in cybersecurity

The growing complexity of cyberspace is exacerbating cyber inequity, widening the gap between large and small organizations, deepening the divide between developed and emerging economies, and expanding sectoral disparities.[1]

Some **35%** of small organizations believe their cyber resilience is inadequate, a proportion that has increased sevenfold since 2022. By contrast, the share of large organizations reporting insufficient cyber resilience has nearly halved.

FIGURE B | Organizations reporting insufficient cyber resilience



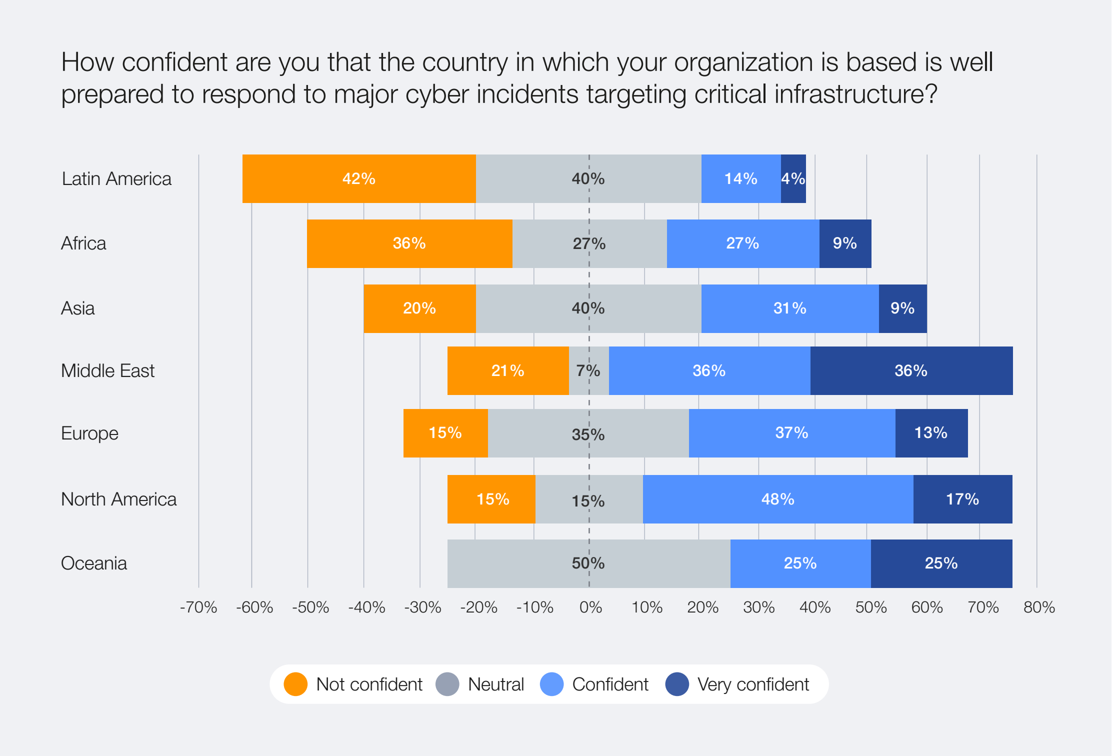
71% of cyber leaders at the Annual Meeting on Cybersecurity 2024 believe that small organizations have already reached a critical tipping point where they can no longer adequately secure themselves against the growing complexity of cyber risks

This disparity in cyber resilience is further highlighted by regional differences in preparedness: while only **15%** of respondents in Europe and North America lack confidence in their country's ability to respond to major cyber incidents targeting critical infrastructure, this proportion rises to **36%** in Africa and **42%** in Latin America.

The public sector is disproportionately affected, with **38%** of respondents reporting insufficient resilience, compared to just **10%** of medium-to-large private-sector organizations. This inequity extends to the cyber workforce, with **49%** of public-sector organizations indicating they lack the necessary talent to meet their cybersecurity goals – an increase of **33%** from 2024.

The *Global Cybersecurity Outlook 2025* report includes a deeper analysis of the most important drivers of complexity and provides valuable insights into the most pressing cyber challenges in the year ahead and their potential implications for executives.

FIGURE C | Regional differences in cyber resilience



These are the key findings from this year's report and the main trends that executives will need to navigate in 2025:

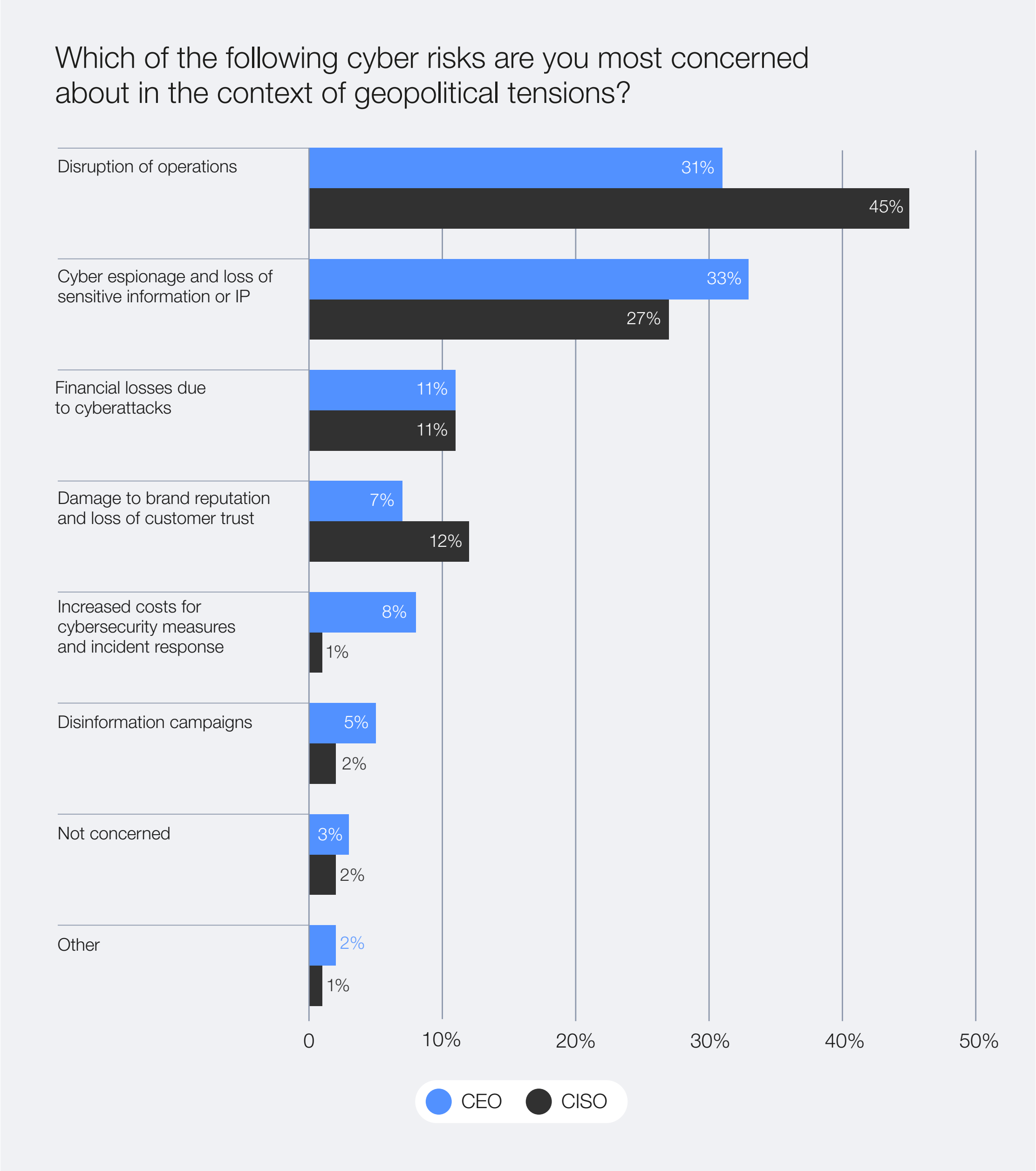
Supply chain vulnerabilities are emerging as the top ecosystem cyber risk

Of large organizations, **54%** identified supply chain challenges as the biggest barrier to achieving cyber resilience. The increasing complexity of supply chains, coupled with a lack of visibility and oversight into the security levels of suppliers, has emerged as the leading cybersecurity risk for organizations. Key concerns include software vulnerabilities introduced by third parties and propagation of cyberattacks throughout the ecosystem.

Geopolitical tensions shape cybersecurity strategy

Nearly **60%** of organizations state that geopolitical tensions have affected their cybersecurity strategy. Geopolitical turmoil has also affected the perception of risks, with one in three CEOs citing cyber espionage and loss of sensitive information/ intellectual property (IP) theft as their top concern, while **45%** of cyber leaders are concerned about disruption of operations and business processes.

FIGURE D **The effects of geopolitical tensions on organizations' cybersecurity strategies**

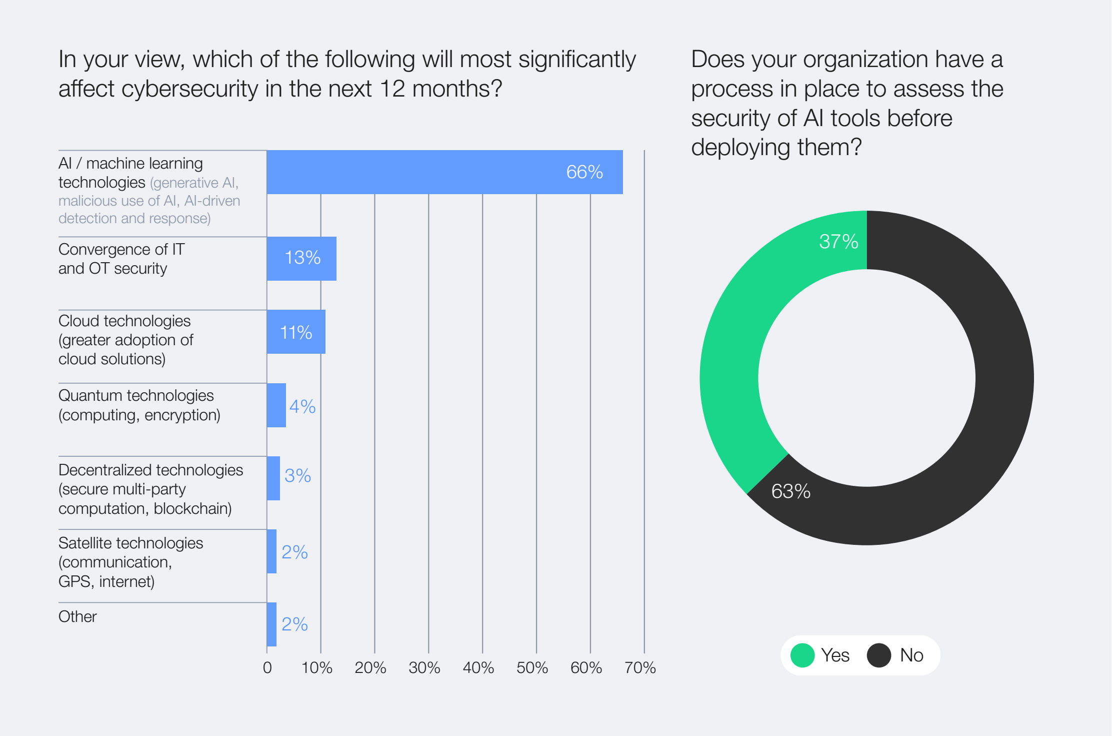


Rapid adoption of AI introduces new vulnerabilities

While **66%** of organizations expect AI to have the most significant impact on cybersecurity in the year to come, only **37%** report having processes in place to assess the security of AI tools before deployment. This reveals the paradox of the gap between the recognition of AI-driven cybersecurity risks and the rapid implementation of AI without the necessary security safeguards to ensure cyber resilience.

FIGURE E

Cybersecurity vulnerabilities anticipated in 2025



Generative AI is augmenting cybercriminal capabilities, contributing to an uptick in social engineering attacks

Some **72%** of respondents report an increase in organizational cyber risks, with ransomware remaining a top concern. Nearly **47%** of organizations cite adversarial advances powered by generative AI (GenAI) as their primary concern, enabling more sophisticated and scalable attacks. In 2024 there was a sharp increase in phishing and social engineering attacks, with **42%** of organizations reporting such incidents.

Regulations bolster cyber resilience, yet their fragmentation introduces significant compliance challenges

Regulations are increasingly seen as an important factor for improving baseline cybersecurity posture and building trust. However, their proliferation and disharmony are creating significant challenges for organizations, with more than **76%** of chief information security officers (CISOs) at the World Economic Forum's Annual Meeting on Cybersecurity in 2024 reporting that fragmentation of regulations across jurisdictions greatly affects their organizations' ability to maintain compliance.

Organizations are grappling with a shortage of critical cyber talent

Since 2024, the cyber skills gap has increased by **8%**, with two out of three organizations reporting moderate-to-critical skills gaps, including a lack of essential talent and skills to meet their security requirements. Furthermore, only **14%** of organizations are confident that they have the people and skills they need today.

1 Understanding complexity in cyberspace

As cyberspace becomes increasingly complex, it has the potential to exacerbate cyber inequity for organizations that are unable to meet growing challenges.

Cybersecurity is entering an era of unprecedented complexity. Geopolitical tensions are intensifying, new technologies are emerging at breakneck speed and threats are evolving into ever more sophisticated attack vectors. At the same time, expanding regulatory demands, vulnerabilities in interwoven supply chains and a widening cyber skills gap are compounding the challenges organizations face in staying secure. The stakes have never been higher.

1.1 Major disparities and disruptions

72%

of GCO survey respondents reported a rise in cyber risks.

The *Global Cybersecurity Outlook 2024* revealed significant cyber inequity, exposing stark disparities in resilience between small and large organizations.[2] The World Economic Forum's *Global Risks Report 2024* found that cyber insecurity is a global risk over multiple time horizons, with cyber risks such as malware, deepfakes and misinformation threatening supply chains, financial stability and democratic systems.[3] Additionally, the *Chief Risk Officers Outlook* from October 2024 ranked cyber risk among the top three threats severely affecting organizations.[4] A striking 71% of chief risk officers anticipated severe organizational disruptions due to cyber risks and criminal activity.[5]

In 2024 the world witnessed the largest IT outage in history, disrupting airlines, banks, broadcasters, healthcare providers, retail payment systems and ATMs globally and causing an estimated $5 billion in losses.[6] This incident underscored the vulnerabilities stemming from dependence on a limited number of critical providers. Cyberthreats continued to escalate, with 72% of respondents to the *Global Cybersecurity Outlook* (GCO) survey (see Appendix: Methodology) reporting a rise in cyber risks. The survey further revealed that cybercrime grew in both frequency and sophistication, marked by ransomware attacks, AI-enhanced tactics – such as phishing, vishing and deepfakes – and a notable increase in supply chain attacks.

1.2 The challenge for the year ahead

The 2025 report finds that a series of compounding factors are driving an escalating complexity in the cyber landscape:

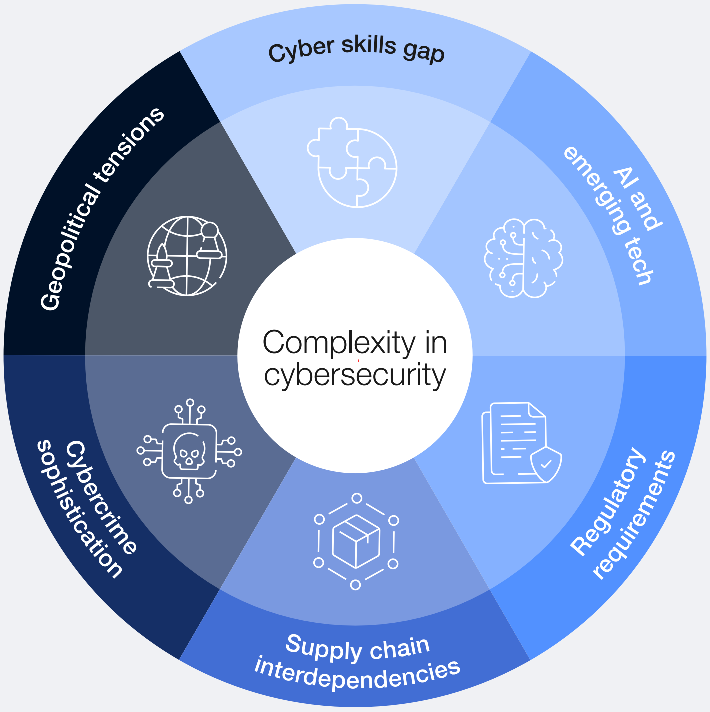
- Geopolitical tensions are contributing to a more uncertain environment.
- Increased integration and dependence on more complex supply chains are leading to a more opaque and unpredictable risk landscape.
- The rapid adoption of emerging technologies is contributing to new vulnerabilities and new threats.

Meanwhile, the proliferation of international regulatory requirements adds an additional compliance burden for organizations. All of these challenges are compounded by a widening skills gap, further complicating the ability to manage cyber risks effectively.

Together, these factors drive increasing complexity and unpredictability in the cyber landscape, which affects organizations in many ways. First, it drives inequity throughout the cyber ecosystem, undermining resilience by creating a divide between those organizations that have the resources to adapt and those that do not and subsequently fall behind. This affects the resilience of the ecosystem, because many larger and more mature organizations typically depend on extensive networks of smaller, often less-mature suppliers, and any incident affecting them could also impact the entire supply chain. Second, it drives greater demand for more specialist skills in cybersecurity, further exacerbating the skills gap. Keeping up with technological advances requires more specific skills that are in greater demand in the cyber skills market. At the same time, complexity puts increasing pressure on often already stretched cybersecurity teams.

These challenges demand a comprehensive re-evaluation of cyber strategies at the organizational and ecosystem level to address the complexity that has become inherent in the cyber landscape.[7] A broader understanding of cyber risk is necessary that goes beyond mere "IT" and considers cyber from an overall business risk perspective.

FIGURE 1 Factors compounding the complex nature of cybersecurity


Cyber skills gap
AI and emerging tech
Regulatory requirements
Supply chain interdependencies
Cybercrime sophistication
Geopolitical tensions
Complexity in cybersecurity

> Against a backdrop of growing cyberthreats and expanding attack surfaces, network defenders are drowning in the operational complexity of a legacy security mindset. They struggle to stitch together dozens of disparate security solutions and enforce security policies across an enterprise's network, cloud and endpoint environments. As a result, people – our most precious cyber resource – are left manually triaging alerts from increasingly automated attacks. To stay ahead of adversaries, we need to reimagine cybersecurity operations, leverage the power of AI and deprive attackers of any technological advantage.
>
> Nikesh Arora, Chairman and Chief Executive Officer, Palo Alto Networks

FIGURE 2 Cybersecurity is becoming increasingly complex

Geopolitical tensions

Geopolitical tensions are an influence on cyber strategy in nearly 60% of organizations, with one in three CEOs citing cyber espionage and loss of sensitive information/IP as top concerns.

Cybercrime sophistication

72% of respondents say cyber risks have risen in the past year, with cyber-enabled fraud on the rise, an increase in phishing and social engineering attacks and identify theft becoming the top personal cyber risks.

Supply chain interdependencies

With 54% of large organizations citing third-party risk management as a major challenge, supply chain challenges remain a top concern for achieving cyber resilience.

Regulatory requirements

78% of leaders from private organizations feel that cyber and privacy regulations effectively reduce risk in their organization's ecosystems. However, two-thirds of respondents cited the complexity and proliferation of regulatory requirements as a challenge.

AI and emerging tech

66% of respondents believe that AI will affect cybersecurity in the next 12 months, but only 37% have processes in place for safe AI deployment.

Cyber skills gap

The cyber skills gap has widened since 2024, with two in three organizations reporting moderate-to-critical skills gaps. Only 14% of organizations are confident that they have the people and skills required.

2 Decoding complexity

As cybercriminals embrace advanced tools, the evolving threat landscape demands innovative strategies to combat increasingly sophisticated and far-reaching attacks.

2.1 The cyberthreat landscape

The evolution of cybercrime

Ransomware remains the top organizational cyber risk year on year, with 45% of respondents ranking it as a top concern in this year's survey. According to leaders at the Annual Meeting on Cybersecurity 2024, significant innovations in ransomware attacks should be expected. This is compounded by the continued adoption of Ransomware-as-a-Service (RaaS), entrenching the commoditization of the ransomware model.[8]

Cyber-enabled fraud ranks as the second-highest organizational cyber risk for 2025, viewed by CEOs as a significant threat alongside ransomware and supply chain disruptions. At the same time, identity theft climbs to the top of the agenda, emerging as the primary personal cyber risk for both CISOs and CEOs.

FIGURE 3 **Organizational cyber risks ranked – 2025**

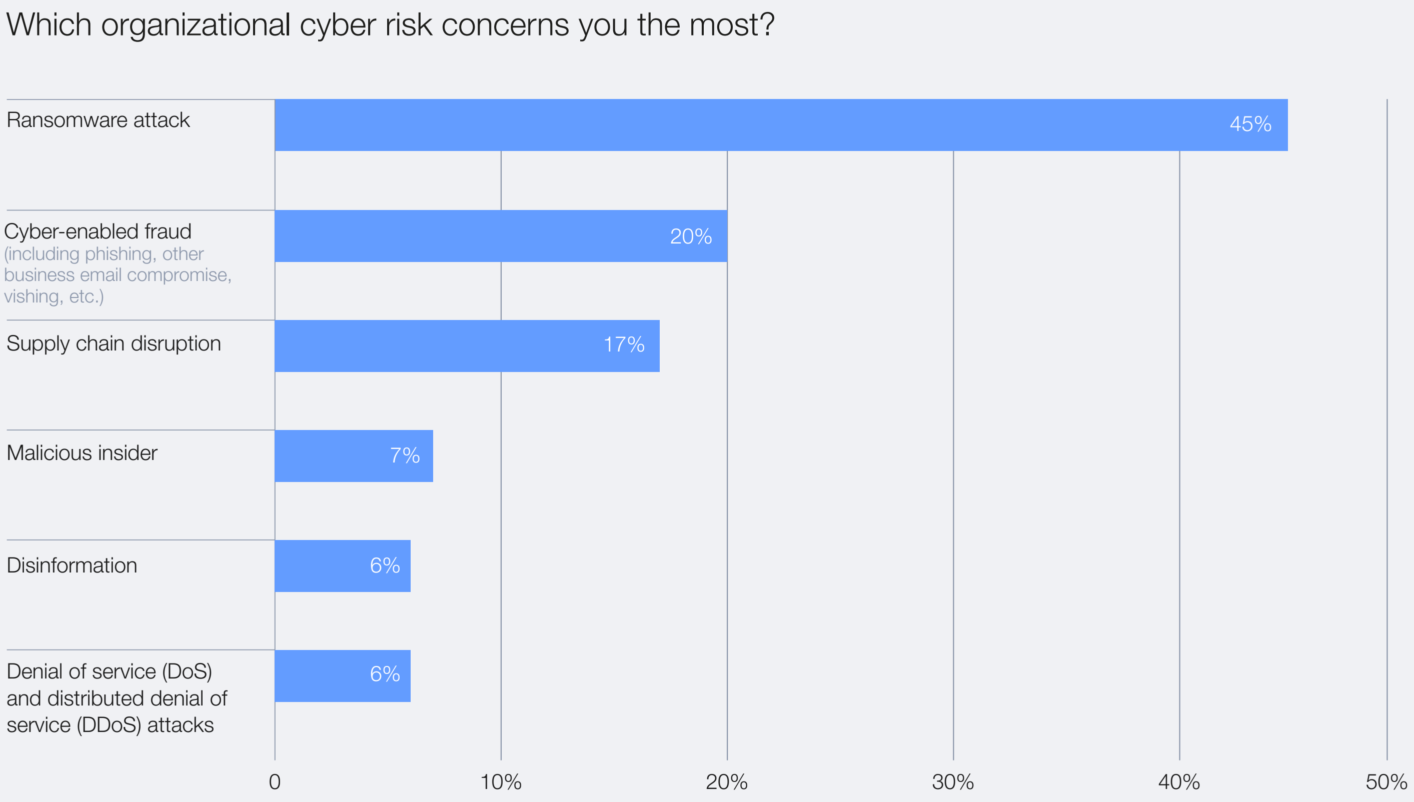


FIGURE 4 Organizational cyber risk – CEO and CISO views

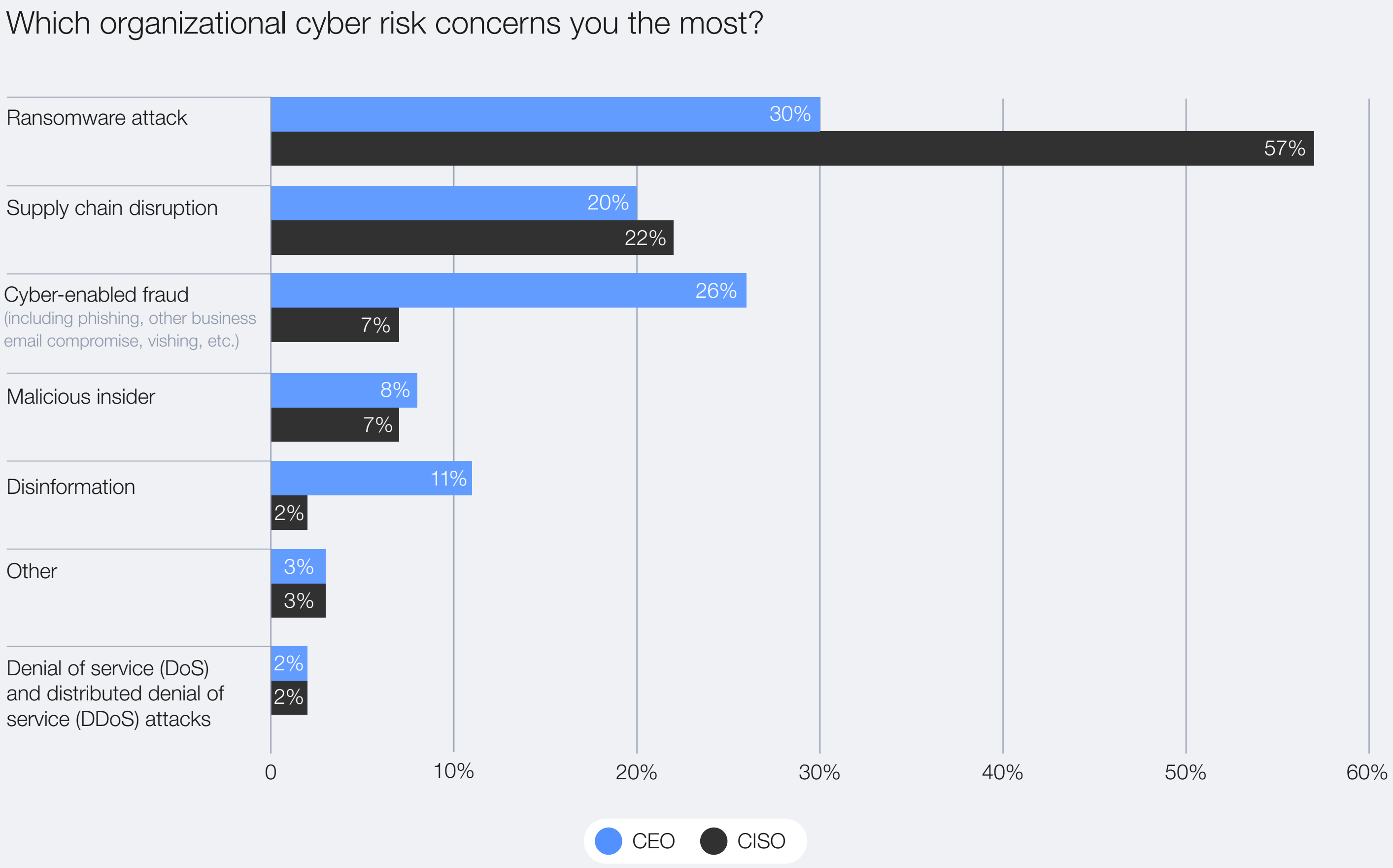
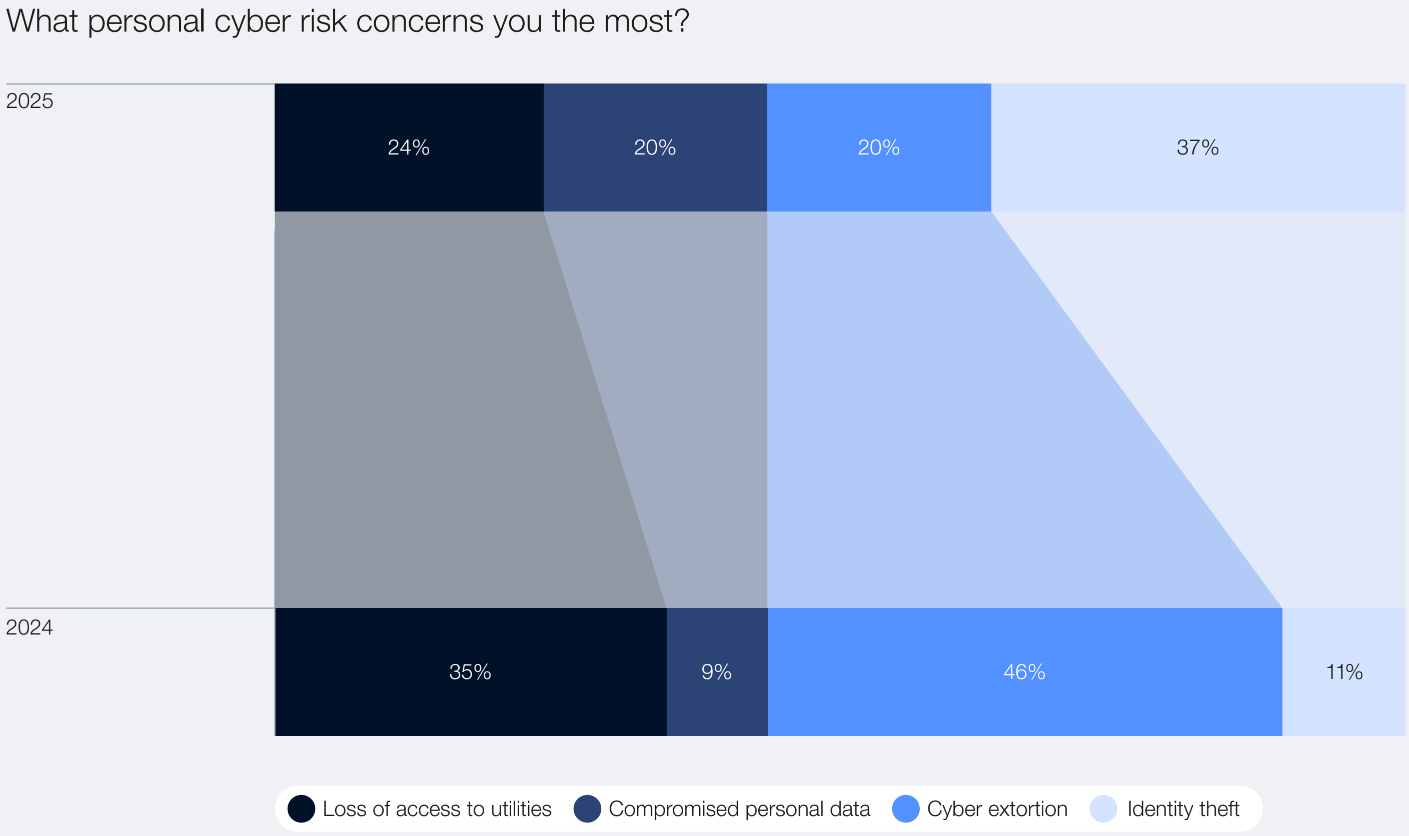


FIGURE 5 Changes in view of personal cyber risk, 2024–2025



> **The rapid advancements and increasing adoption of digital platforms globally is matched by an equally evolving cyberthreat landscape. Cybercrime today is increasing not just in scale but also in sophistication. As our digital footprints widen, so does the potential attack surface for nefarious actors. It is essential that we work together to address this growing menace. The borderless nature of the internet necessitates collaboration across various jurisdictional limitations to ensure that threat actors have no safe haven for their evil activities.**
>
> Ivan John E. Uy, Secretary of Information and Communications Technology of the Philippines

Cyberattackers are adopting new tools to increase the effectiveness and scope of familiar forms of attack, such as ransomware and business email compromise (BEC). GenAI tools are lowering the cost of the phishing and social engineering campaigns that give attackers access to organizations. Therefore, while the core character of cyberattacks has remained stable, organizations may need to place additional emphasis on protecting themselves against well-developed phishing and cyber-fraud campaigns.

Cybercrime-as-a-Service (CaaS) platforms continue to be a dominant and rapidly growing business model in the criminal landscape, allowing individuals or groups without technical expertise to engage in illicit online activities by purchasing the necessary tools and support.[9] This model, which is already well established among criminal groups, has progressively been adopted in other areas of cybercrime, such as AI-enhanced phishing attacks. These platforms present a challenge, as they remove the barriers for entry into cybercriminal activities. While progress has been made in dismantling some of the platforms, enforcement efforts remain inconsistent as CaaS platforms continue to thrive.

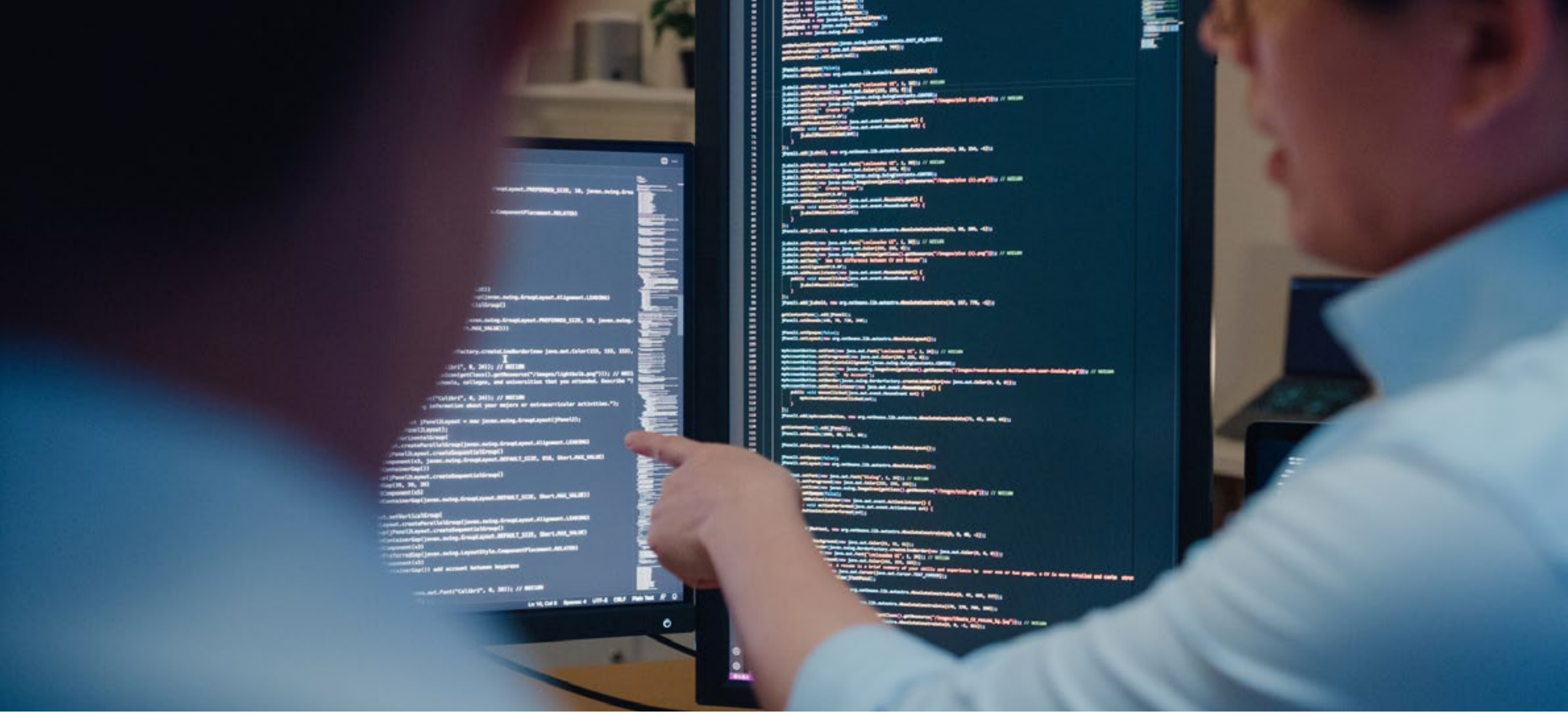
The convergence of cybercrime and organized crime groups

The surge in the volume and value of cyber-enabled fraud has attracted “traditionally” violent organized crime groups into the cybercrime market. The interaction of organized cybercrime with organized violent crime groups is changing the nature of cybercrime and greatly increasing their social impact.

This is perhaps most starkly shown by the trafficking of more than 220,000 people to forcibly work in online scam-farms in South-East Asia.[10] With such farms engaging in the harvesting of data, disinformation and social engineering to name a few capabilities, they are essentially becoming “criminal service providers”.[11] 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).[12]

The entry of traditional organized crime groups into the cybercrime arena changes the character of the criminal market. Organized crime groups are accustomed to causing physical harm and are arguably less concerned about the risk created by attacking critical social services such as medical services.[13] When this cultural change is paired with the scale provided by CaaS platforms, the range of organizations that could be targeted by attacks such as ransomware becomes wider.[14]

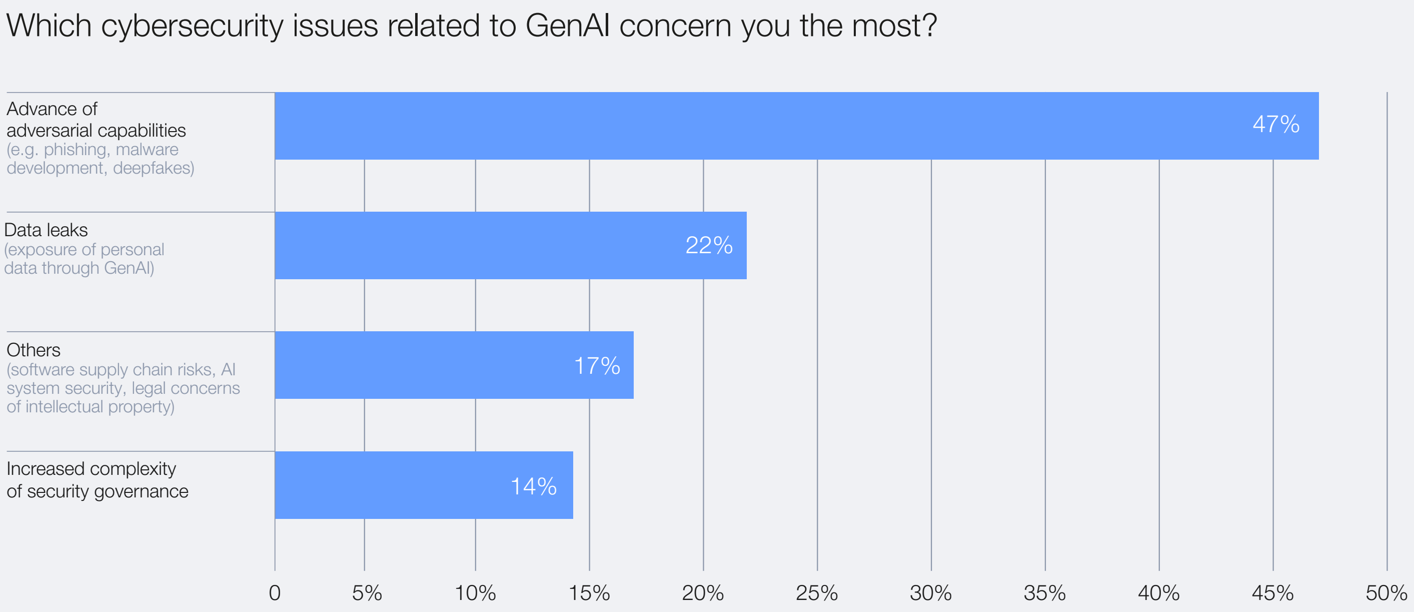
> **Cybercrime has persistently evolved alongside the threat landscape, and its reach extends beyond financial loss, becoming a disruptive force that threatens our societies. We must remain vigilant and collaborate across sectors to safeguard the future of our digital world. Cybercrime’s impact is far-reaching – it can halt operations, undermine confidence and permeate to our operational technology and critical infrastructure. In the year ahead, we must prioritize not only defence but proactive and systemic disruption of these criminal networks as part of our collective effort to ensure cyber resilience and protect our digital future.**
>
> Ken Xie, Founder, Chairman of the Board and Chief Executive Officer, Fortinet



AI as a catalyst of cybercrime

GenAI tools are reshaping the cybercrime landscape by enabling criminals to refine their methods, and automate and personalize their techniques. With 47% of organizations citing their top concern surrounding GenAI as the advance of adversarial capabilities, cybercriminals are harnessing the efficiency of AI to automate and personalize deceptive communications. Some 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.

FIGURE 6 **Cybersecurity issues linked to GenAI**



Cybercriminals are using GenAI to convincingly replicate the communication styles of an organization's senior leaders. These tools harness contextual data from sources such as social media, public statements or leaked documents, making social engineering attempts much more sophisticated and challenging to identify. GenAI also supports attackers in developing credible social engineering attacks in a wider range of languages, which helps threat actors target a greater number of people in more countries at a lower cost.

When augmented with GenAI, threat actors can create convincing impersonations of the voice, video, images and writing styles of senior leaders. When these deepfakes are maintained over prolonged interactions with targeted staff, they can be used to defraud organizations or help attackers gain access to their IT systems. Accenture's research has noted a 223% rise in the trade of deepfake-related tools on dark web forums between Q1 2023 and Q1 2024.[15]

Additionally, 55% of CISOs polled during the Annual Meeting on Cybersecurity 2024 stated that deepfakes pose a moderate-to-significant cyberthreat to their organization. With staff remaining the real target of deepfake attacks, as well as phishing campaigns in general, organizations will need to rethink how they train and protect everyone, from employees to the C-suite and board, about new patterns of cybercrime.

> **As global leaders, we see cyber challenges as more than just a threat – they're a chance to make a real difference in how we protect people and businesses. Malicious cyber activity takes a significant toll on the most vulnerable populations, so we must urgently drive ecosystem-level solutions that bring everyone together, from small local companies to big global corporations. By collaborating like never before, we can turn the tables in 2025, make systemic change and create digital defences that work for everyone.**
>
> Philip Reiner, Chief Executive Officer and Founder,
> Institute for Security and Technology

Finally, GenAI lowers the barriers to entry into the cybercrime arena in terms of cost and required expertise. GenAI is expected to streamline the process from the exploitation of vulnerabilities to the deployment of malware, scaling up operations that were previously reliant solely on human capabilities.

By understanding the complexity of the cyberthreat landscape as well as the behaviour and motivations of cybercriminals, organizations can better assess the risks facing them and then tailor and prioritize security strategies to enhance resilience against such threats.

> **The complexity of today's cyber threats and evolving criminal methodologies requires a unified response. This response requires coordination not only from the global law enforcement community, but with cybersecurity experts who provide their own talents, experiences and expertise. In 2024, INTERPOL's Cybercrime Directorate supported several regional and global cybercrime operations that were very successful in large part due to these collaborations. As we move into 2025, our team will continue to pursue new partnerships and strengthen existing ones to have even greater impact disrupting cybercriminal activity.**
>
> Neal Jetton, Director, Cybercrime Directorate, International
> Criminal Police Organization (INTERPOL)

CASE STUDY 1

Old scams and new technology – Arup

Arup hit the headlines for the wrong reasons when the firm was targeted by criminals who succeeded in pulling off a major fraud. "Fraudsters use deepfake technology to trick employee into paying millions" ran one headline, but the story is more subtle than that.

Clearly, media attention was driven by the fact that the fraudsters used manipulated videos and voicemails to convince people they were talking to genuine colleagues. But as Arup's Chief Information Officer, Rob Greig, pointed out, the interesting part is that the criminals did not penetrate the firm's IT networks or disrupt business operations. Rather, they used "technology enhanced social engineering" to convince people to process transactions.

It was a sophisticated, preplanned attack that used tactics such as phishing, vishing and smishing, all backed by fake documentation and a false sense of urgency. At its heart, though, this was an old-fashioned payment scam with a modern makeover.

Since the incident, the firm has reviewed every aspect of its systems and processes. Among the key lessons learned is that cybersecurity alone is not enough. Building real resilience requires a culture of critical assessment and the ability to spot red flags across the organization.

The most important lesson, though, is that industry, the police and public authorities all need to find better ways to share information and frustrate the fraudsters.

Beyond cybercrime: Emerging threats to critical infrastructure and human safety

> **With emerging technologies reshaping the landscape, cyber is no longer limited to the CIA triad: confidentiality, integrity and availability of information. Cybersecurity now encompasses human safety and needs to address the real risk to people's lives when a system is attacked or compromised.**
>
> Bushra AlBlooshi, Director of Cybersecurity Governance Risk Management Department, Dubai Electronic Security Centre

Escalating geopolitical tensions and increasingly sophisticated cyberthreats pose significant risks to critical infrastructure, which depends on networks of interconnected devices and legacy systems. The ongoing conflict in Ukraine exemplifies these vulnerabilities, with critical sectors such as energy, telecommunications, water and heating repeatedly targeted by both cyber and physical attacks.[16] These attacks often focus on disrupting control systems and compromising data, highlighting the critical risks associated with operational technology (OT). As cyberthreats continue to evolve, they not only threaten system functionality but also jeopardize human safety, increasing the severity and consequences of disruptions to vital infrastructure. Some critical, high-risk areas to monitor are:

Water facilities

Cyberattacks on water facilities pose significant risks to public safety, infrastructure and national security. The Cybersecurity and Infrastructure Security Agency (CISA) of the United States outlined these risks in a toolkit, emphasizing the vulnerabilities in OT systems used in water facilities, such as remote access points and outdated software.[17] Cybercriminals can exploit these weaknesses to disrupt water-treatment processes, causing potential contamination, loss of service or other hazardous consequences. A notable example of these threats occurred in October 2024, when a cyberattack targeted the largest water utility in the United States, disrupting operations and raising alarms about the security of critical infrastructure.[18]

Biosecurity

Rapid technological advances have redefined the biological threat landscape, with biosecurity coming to the forefront. The World Health Organization (WHO) has warned that advances in artificial intelligence, cyberattacks and genetic engineering could pose potentially catastrophic risks to global biosecurity.[19] A 2024 WHO report highlighted several ways in which cyberthreats could compromise biosecurity, including accessing sensitive data or research, disruption of laboratory security systems, theft or sabotage of biosecurity-relevant information and espionage for competitive or harmful objectives.[20] Furthermore, cyberattacks could incapacitate essential laboratory systems, interrupting operations and causing loss of data integrity, which would delay critical research or compromise safety protocols. Over the course of 2024, two laboratories were targeted in South Africa and the United Kingdom.[21] These vulnerabilities underscore the need for advanced cybersecurity measures in biosecurity strategies to address these growing risks.

Simultaneously, the sensitive nature of genomic data poses new risks due to its unique qualities, such as the ability to identify individuals and reveal their familial ties.[22] These characteristics expose genomic data to threats such as reidentification from seemingly anonymous datasets, unauthorized access leading to privacy violations and potential misuse. The breach of a genetic-testing company in late 2023 that exposed the data of nearly 7 million people has already trained the spotlight on these risks.

> **As genomics continues to evolve as a critical field, securing sensitive biological data, the interconnected systems and the users becomes essential. The protection of bioinformatics platforms, along with the prevention of misuse in biotechnical applications, is vital. This includes safeguarding data analytics and securing the broader ecosystem of interconnected systems to mitigate risks across sectors. As these emerging technologies grow, the need for robust security in bioinformatics, their analytics and cyber-physical systems will only increase, creating new resiliency challenges for cybersecurity leaders.**
>
> Hoda Al Khazimi, Director, Centre for Cybersecurity, New York University Abu Dhabi

Communications infrastructure

From large-scale state-sponsored cyber espionage via telecommunications infrastructure to the targeting of satellites and undersea cables, geopolitical tensions continue to manifest through the increasing number of attacks on critical communications infrastructure.[23]

Following the 2022 attack on ViaSat's satellite network that highlighting the consequences of a cyberattack on military communication and civilian life in Europe, there were 124 further recorded cyber operations against the space sector in the context of the conflict in Ukraine.[24] With the increased reliance on space technologies, it is a prime target for espionage, operational disruption and weaponization.

Undersea cables are crucial for global data flow and economic exchange. Their strategic role makes them vulnerable to monitoring and disruption, especially with limited defence measures and rising geopolitical tensions. Incidents in the Baltic Sea since the start of the conflict in Ukraine highlight the urgent need to protect these critical pieces of infrastructure.[25]

Climate and energy

As the global climate crisis intensifies, its implications for cybersecurity are becoming increasingly significant. Modern technology relies heavily on substantial energy consumption, rendering power grids highly attractive targets for cybercriminals. Simultaneously, energy systems are undergoing a profound transformation as societies transition to renewable technologies. It is essential that these emerging energy systems are designed with security as a foundational priority; otherwise, in the effort to address an existential crisis with urgency, there is a risk of introducing vulnerabilities that could undermine the reliability of this new energy infrastructure, with far-reaching consequences for the economy and society.

2.2 Security in the Intelligent Age

> **The security of AI systems (or lack thereof) can have far-reaching implications given the increasing adoption of AI. My belief is that AI should be developed and deployed in a safe, secure and trustworthy manner for the public good. Advancing this will need an inclusive, multilateral and multistakeholder approach. Digital technology like AI is borderless and global. We must cooperate and work together to secure AI, even in the face of ongoing geopolitical tensions and strategic competition in critical and emerging technologies.**
>
> David Koh, Commissioner of Cybersecurity and Chief Executive, Cyber Security Agency of Singapore (CSA)

"The Intelligent Age – driven by rapid advancements in AI, quantum computing and blockchain – is transforming everything and changing it right now, in real time." The advent of the Intelligent Age brings unprecedented opportunities and unprecedented risks; the importance of security in safeguarding the promise of these transformative technologies cannot be overstated. [26]

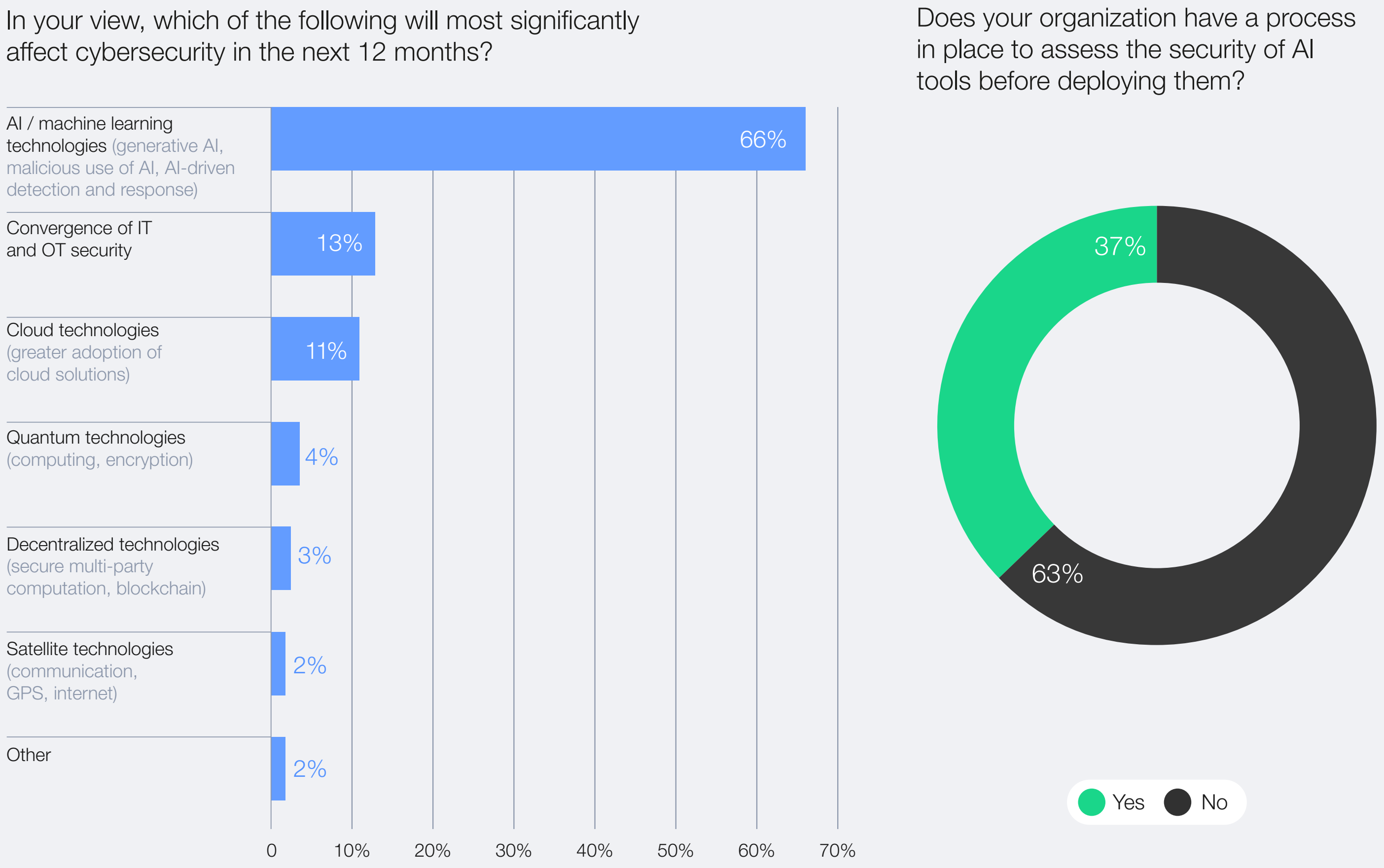
The AI–cyber paradox

Emerging technologies present significant opportunities for organizations to enhance efficiency and optimize operations. As a result, many organizations are actively developing strategies to integrate these technologies into their infrastructure. However, the cyber risks associated with the underlying technologies or their implementation in organizations often do not receive the attention and consideration they require.

While AI is not a new phenomenon, the advent of GenAI has accelerated the adoption of AI in organizations around the globe. Organizations are testing or adopting AI technologies to drive efficiencies and gain a competitive advantage. However, they do not always design strategies and processes for secure implementation. When adopting new technologies, it is critical for organizations to assess the cyber risks they entail and implement the related cybersecurity controls to ensure operational and wider business cyber resilience.

According to the GCO survey, 66% of organizations anticipate that AI will have the most significant impact on cybersecurity in the coming year. However, only 37% of respondents report having a process in place to assess the security of AI tools prior to deployment. This creates a risk that organizations may implement or adopt AI systems – whether developed internally or sourced from third-party providers – without fully considering the associated cybersecurity risks and associated mitigation measures, while potentially introducing vulnerabilities into their IT estate.

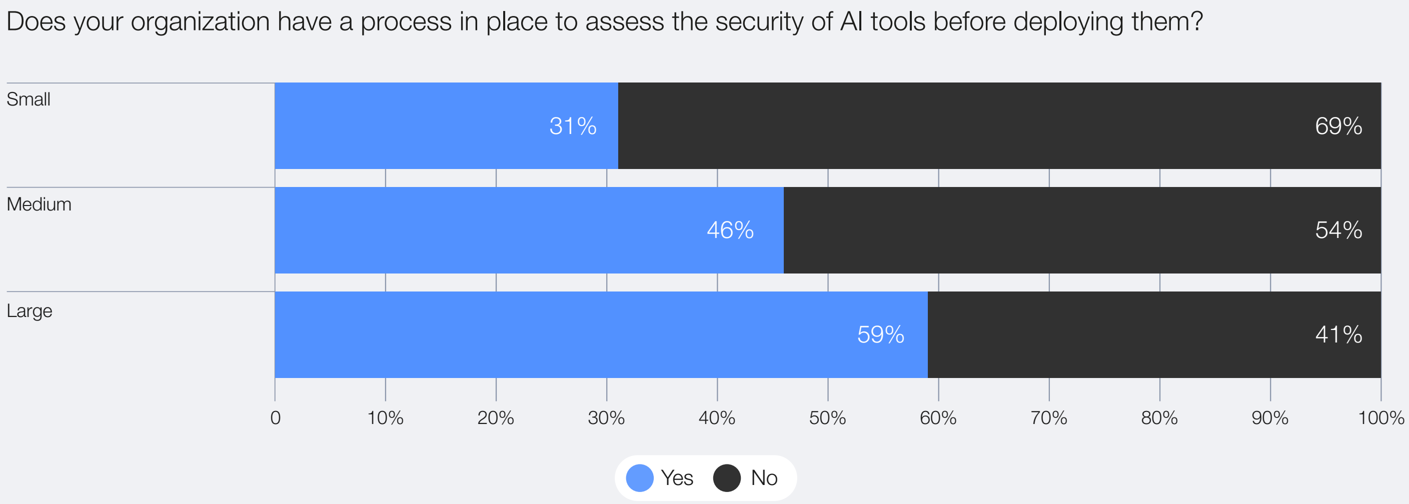
FIGURE 7 **Cybersecurity vulnerabilities in 2025 predicted by professionals**



This issue is particularly alarming for smaller organizations, of which 69% lack adequate safeguards for the secure deployment of AI technologies. These could include, for example, ensuring all new assets (devices and software) relating to AI infrastructure are inventoried, ensuring the security of training data and monitoring the behaviour of AI systems to detect manipulation in a timely manner.[27] This contributes to the widening of cyber inequity as it leaves less-resourced entities more exposed to the risks of insecure AI models. It also increases the collective vulnerability of the ecosystem in which these smaller organizations operate.

A holistic approach is necessary for the secure adoption of AI: 74% of global CEOs surveyed by KPMG agree that building a strong cyber culture is central to integrating AI safely into their organization.[28]

FIGURE 8 **Larger organizations are more likely to have AI security procedures in place**



> **The LLMs currently in use are constitutively insecure, and the adversarial attacks and supply chain sabotage that are possible are not being addressed in a sufficiently meaningful way. Integrating these models into critical infrastructure before such attack vectors are remedied is dangerous and needs to be reevaluated.**
>
> Meredith Whittaker, President, Signal

BOX 1 ***Artificial Intelligence and Cybersecurity: Balancing Risks and Rewards***

The AI Governance Alliance, launched by the World Economic Forum in June 2023, seeks to provide guidance on the responsible design, development and deployment of artificial intelligence systems. Its report, *Artificial Intelligence and Cybersecurity: Balancing Risks and Rewards*, equips top leaders with a set of questions that can help them define and communicate the key parameters within which decision-making on AI adoption and its associated cybersecurity can be made:

1. Has the right risk tolerance for AI technologies been set, and is it understood by all risk owners?

2. Is there a proper balancing of risks against rewards when new AI projects are considered?

3. Is there an effective process in place to govern and keep track of the deployment of AI projects within the organization?

4. Is there a clear understanding of organization-specific vulnerabilities and cyber risks related to the use or adoption of AI technologies?

5. Is there clarity on which stakeholders within the organization need to be involved in assessing and mitigating the cyber risks from AI adoption?

6. Are there assurance processes in place to ensure that AI deployments are consistent with the organization's broader organizational policies and legal and regulatory obligations – for example, relating to data protection or health and safety?

AI for cyber defence

AI holds the promise of transforming methods to defend against cyberthreats. It can give defenders the upper hand – with advanced tools able to quickly spot and respond to dangers – if they can keep up with the pace of AI integration. Simply put, AI can augment human abilities, making cyber defence stronger and more efficient.

AI is transforming cybersecurity by reducing toil and freeing up manpower, enabling systems to process vast amounts of data for early threat detection and uncovering hidden risks. This technology can enhance threat alert triage, prioritization, anomaly detection and pattern recognition. It can also classify vulnerabilities, automate patching, accelerate data processing and manage configurations.[29] Moreover, AI can serve as a security adviser – like an "AI-CISO" or "virtual CISO" – improving software security and optimizing decision-making to make the most of limited resources. Given recent advances in AI agents, resource optimization and autonomous assistants that can help defenders to this end may certainly be on the horizon.[30]

Large language models (LLMs) also offer the opportunity to collect richer intelligence, powering the threat-intelligence cycle. AI models can analyse and categorize the types of questions attackers ask, their interaction patterns and even linguistic markers that might identify specific groups or individuals. This data can then feed back into threat-intelligence systems, refining detection algorithms and providing achievable insights to cybersecurity teams by refining the content analysis and triage stages.[31] Backed by AI and machine learning, defenders can use continuous monitoring and real-time visibility to better identify and address software vulnerabilities such as zero-day threats and exploits. Advanced threat detection systems using behavioural analysis, network segmentation and machine learning can contain potential breaches and limit the persistence of threat actors within compromised environments.

The integration of LLMs into honeypots represents a new frontier in deception-based cybersecurity.[32] By embedding LLMs into these decoy environments, defenders can create sophisticated, dynamic interactions that adapt to adversarial behaviour in real time.[33] At the core of this innovation is the ability of LLMs to simulate human-like responses, making honeypots far more convincing to attackers.

Unlike static systems or preconfigured responses, LLMs can generate contextually appropriate, nuanced dialogues that respond appropriately to attacker queries, prolonging engagement and misleading attackers into thinking they are interacting with legitimate systems. This creates an environment in which malicious actors unknowingly reveal their intent, methods and even operational details while thinking they are making progress in their attack. One notable project, SPHINX, supported by the European Union (EU)'s 2020 Research and Innovation Programme, 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.[34] LLMs can help create realistic "bait" assets, such as fake credentials, plausible system configurations or generated content that mirrors the sensitive data attackers seek. These assets, underpinned by LLMs, help maintain the illusion of authenticity, increasing the likelihood that attackers will stay in the honeypot longer, giving defenders more time to respond.

Preparing for the quantum threat

40%

of organizations are taking proactive steps to understand the quantum threats.

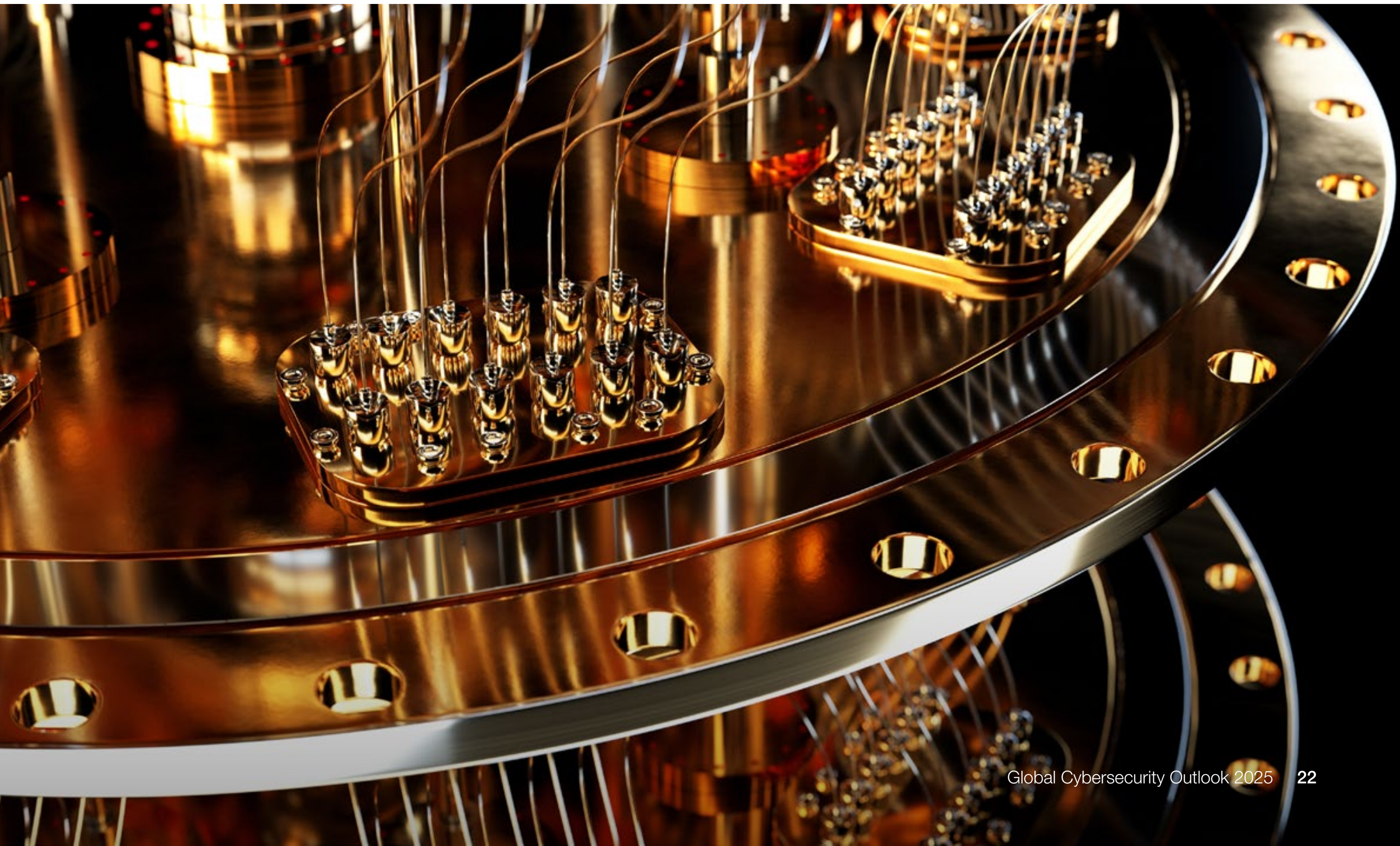
Quantum computing offers significant economic and scientific opportunities by unlocking unprecedented computing power. However, quantum computing advances also accelerate the emergence of security risks, particularly the potential to break public-key encryption, which is vital for securing digital systems such as online banking and government communications. While the timeline for quantum computing's full potential remains uncertain, the associated quantum security risks are already at play.

In a focus group at the 2024 Annual Meeting on Cybersecurity, 40% of organizations indicated that they have started to take proactive steps by conducting risk assessment to understand the quantum threat. Many organizations have been increasingly vigilant about threats such as "Harvest Now, Decrypt Later", where malicious actors collect encrypted data now with plans to decrypt it once quantum computing can break existing encryption, posing significant challenges for both current and future data security. However, some organizations are still awaiting support from industry standards, guidelines and government regulations.

Multiple efforts have been taken to spur action. The G7 Cyber Expert Group identified a list of risks to financial system security, providing governments and central banks with key recommendations while calling for action.[35] The World Economic Forum in collaboration with the Financial Conduct Authority also developed recommendations to inform global regulatory procedures to help ensure a collaborative and globally harmonized approach to quantum security.[36]

Recently, the National Institute of Standards and Cryptography (NIST) released three highly anticipated post-quantum cryptography (PQC) algorithm standards that were built to withstand cyberattacks from quantum computers.[37] Beyond PQC standards, other technologies – quantum key distribution (QKD) and quantum random number generation (QRNG) – have also been garnering attention because they could help mitigate, either individually or in combination, the risk posed by quantum to public-key cryptography.

A successful transition begins with strong cyber foundations and a clear quantum-readiness strategy, emphasizing the need for organizations to begin their quantum-readiness journey today.

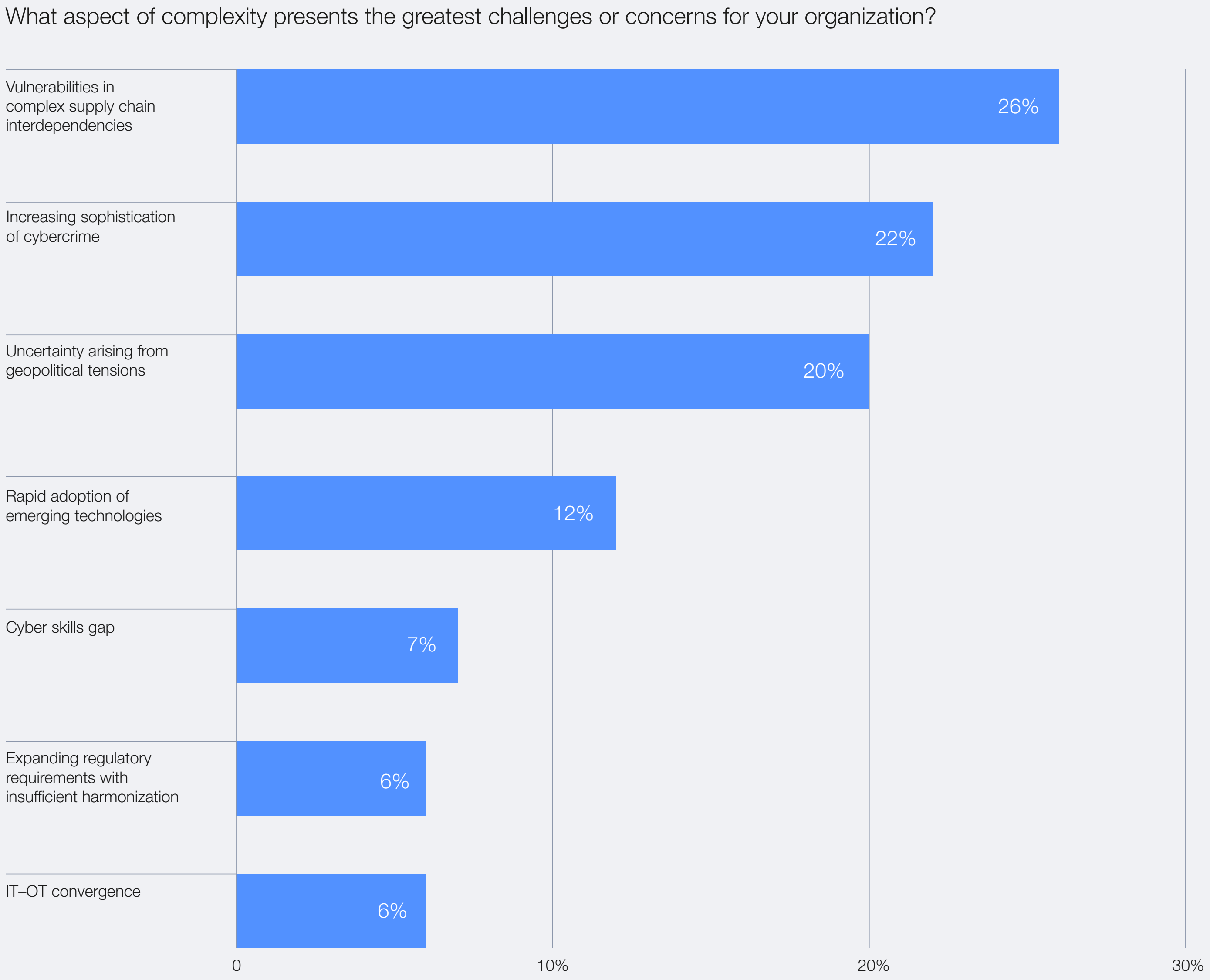


2.3 Growing ecosystem interdependencies and risks

Since the launch of the *Global Cybersecurity Outlook* in 2022, the survey has shown a consistent concern among business and cyber executives about the state of the cyber ecosystem. At the 2024 Annual Meeting on Cybersecurity, cyber experts identified vulnerabilities within interconnected supply chains as the leading contributor to the growing complexity in cyberspace. This year's Outlook will analyse how intricate supply chain dependencies, geopolitical risk, inequity and regulations are affecting the cyber resilience of ecosystems.

> **As digitalization advances, cyber threats are becoming increasingly complex, particularly as interdependencies across third-party supply chains and broader ecosystems grow. Cyber attackers need only succeed once to cause significant harm, while our collective defences – spanning organizations, suppliers and global networks – must be robust and cohesive at all times. To effectively safeguard the energy infrastructure that supplies billions globally, we need closer collaboration and transparency between all stakeholders, both locally and internationally, to mitigate risks across the supply chain and digital ecosystem.**
>
> Amin Nasser, President and Chief Executive Officer, Aramco

FIGURE 9 **Challenges to organizations posed by cybersecurity threats**



The complexity of supply chain interdependencies

The growing complexity of supply chains and the limited control organizations have over them has become a primary concern for executives, emerging as the top cyber risk from an ecosystem perspective. This year, 54% of large organizations highlight supply chain challenges as the greatest barrier to achieving cyber resilience. By comparison, third-party risk management does not feature among the top five concerns for smaller organizations.

TABLE 1 **The main organizational challenges to cyber resilience**

Small organizations	Medium organizations	Large organizations
01 **Complex and evolving threat landscape**	**01** **Complex and evolving threat landscape**	01 Third-party risk management
02 Skills shortage	02 Third-party risk management	**02** **Complex and evolving threat landscape**
03 Lack of incident response preparedness	03 Complexity of environments (e.g. IT, OT, IoT)	03 Complexity of environments (e.g. IT, OT, IoT)

Most of these concerns, according to the GCO survey, are centred on software vulnerabilities introduced by third parties or vendors and cyberattacks, such as malware distribution, that exploit weaknesses in the supply chain. Following the US Executive Order 14028: Improving the Nation's Cybersecurity, which put a strong emphasis on software bill of materials (SBOM),[38] other standards and regulations such as Payment Card Industry Data Security Standard (PCI DSS) and the EU's Cyber Resilience Act introduce SBOM-related requirements in order to allow organizations to better understand, manage and secure their applications.[39]

60%

of organizations reported that their cyber strategies were influenced by geopolitical tensions.

Another important issue is the uncertainty surrounding supply chain interdependencies. Lack of visibility throughout the ecosystem and oversight over the degree of security maturity of their suppliers is a major concern for organizations. At a focus group at the 2024 Annual Meeting on Cybersecurity, 41% of participants expressed the view that enhancing visibility of third-party dependencies is the top priority for improving supply chain cyber resilience. Enforcing security standards on third-party providers – let alone fourth- and Nth-party providers – on whose services they have become dependent, has become increasingly difficult. This is confirmed by the GCO survey: 48% of participating CISOs indicated that ensuring third-party compliance with their security requirements is the main challenge to effectively implementing cyber regulations. This is often compounded by the fact that baseline security requirements at times differ between industries, and it becomes difficult to enforce more onerous requirements throughout the supply chain.

Additionally, organizations find themselves increasingly dependent on a limited number of critical providers that have managed to establish themselves as leaders in their capability. 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. Owing to the complexity of the ecosystem, a cyberattack or outage can have far-reaching and unpredictable consequences. 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.

> **Building resilience is critical in today's interconnected landscape, where supply chain complexity can create innumerable cybersecurity challenges. Smart adversaries exploit third-party vulnerabilities, making collaboration essential. By enforcing standards, leveraging threat intelligence and equipping organizations of all sizes with more effective cybersecurity solutions, we can close gaps and fortify the ecosystem to stop breaches while safeguarding business continuity and digital trust.**
>
> George Kurtz, Founder and Chief Executive Officer, CrowdStrike

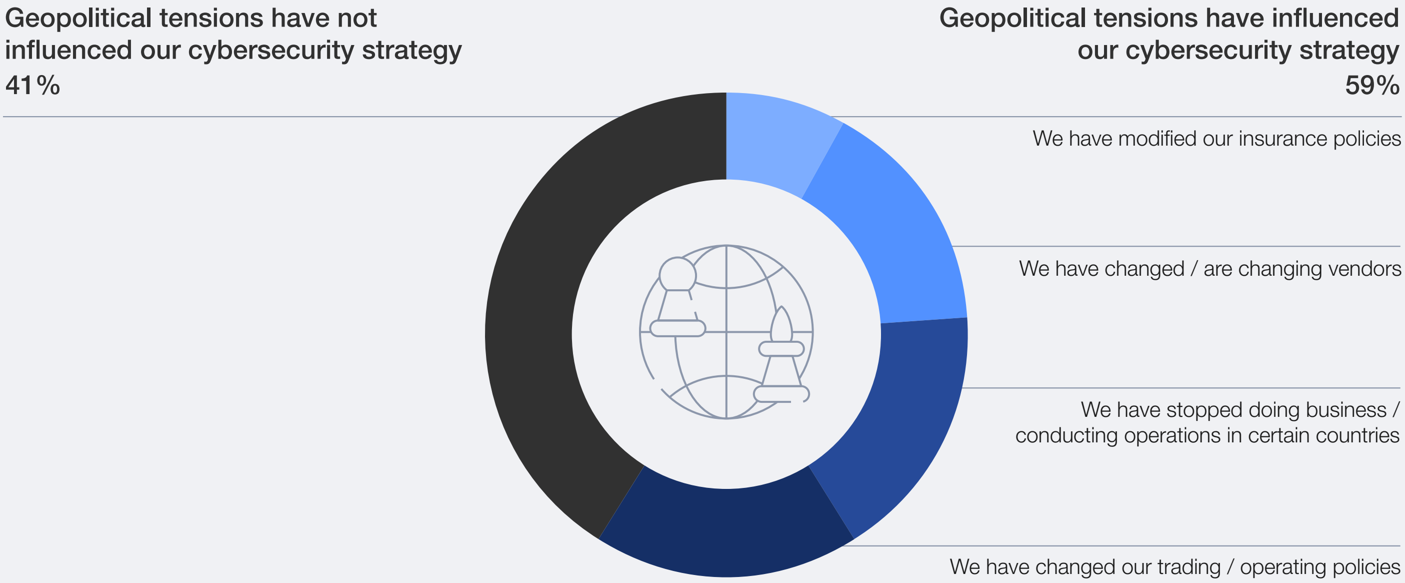
Similarly, cloud providers play a crucial role in enhancing the security of modern ecosystems, offering a stronger security posture than many organizations can achieve on their own. However, individual organizations often have limited control over the cyber risks associated with cloud services and must manage these as part of their broader strategy. Many organizations embrace cloud technologies for their cost efficiency, requiring a clear understanding of the shared responsibility model, where roles and accountability can sometimes overlap. As organizations move more workloads to software-as-a-Service (SaaS) platforms with limited control over configurations, this introduces a significant concentration of risk. A ransomware attack on a major provider could ripple across thousands of dependent businesses, halting operations overnight. While such providers place great emphasis on resilience, no system is infallible. Companies must invest in their own business resilience strategies, ensuring they have contingency plans that do not rely solely on their SaaS partners.

In attempting to address these concerns, some organizations have opted for solutions close to home, including reconsidering risk exposure throughout their entire end-to-end supply chain and enforcing secure software development practices, including robust risk assessment and dependency management. Others pointed to the importance of standardization and certification to increase trust in services provided in the digital ecosystem, while recognizing that financial penalties have the greatest likelihood of providing sufficient incentive. In all, this reflects the sentiment that, while responsibility for secure software development should be clearly defined and transparent to hold developers to account, CISOs must continue to build sufficient resilience into their environments. To support this effort, the EU Cyber Resilience Act, which came into force in the second half of 2024, aims to enhance the cybersecurity of products with digital elements throughout the EU.

The impact of geopolitical risk on ecosystem complexity

The GCO survey finds that nearly 60% of respondents reported that their cyber strategies were influenced by geopolitical tensions. Moreover, ongoing conflicts in 2024 have continued to affect regions beyond those directly involved, with 18% of organizations adjusting trading or operational policies, 17% halting business or operations entirely in certain regions and 16% of organizations reporting changes in vendors.

FIGURE 10 The influence of geopolitical tensions on cybersecurity strategy



Of increasing concern is the spillover from nation-state threats into the cybercriminal domain, whereby nation-state actors increasingly rely on tools and tradecraft from the cybercriminal world and vice versa.[40] In interviews conducted for this report, cyber executives agreed that geopolitical tensions are reshaping the cybersecurity landscape. One CISO emphasized that state-sponsored attackers are increasingly targeting not just governments but are also aiming to disrupt economies, undermine critical infrastructure and create chaos within global systems. Today, organizations face direct attacks but also risk becoming collateral damage, as adversaries exploit vulnerabilities in supply chains and shared services. In this environment, understanding geopolitical dynamics has become crucial for effective long-term risk management.

CISOs recognize this volatile situation and confirm there are no standard playbooks for dealing with geopolitical risk. Rather, the situation calls for a return to old-fashioned risk management, by looking at problems from a business-impact perspective first, before managing and eventually accepting any residual risk. Close alignment between the security function and the business is therefore essential to address today's complexity stemming from geopolitical risk.

CASE STUDY 2

Cybersecuring the Paris Olympic Games

Cybersecuring the Paris Olympic Games was a priority for the French government and took two years of preparation, which included large-scale audits, penetration testing and cyber-crisis management exercises. In the end, despite there being a significant number of cyberattacks – more than any previous Olympic Games – few were successful, and none were able to disrupt the Games or key pieces of infrastructure.

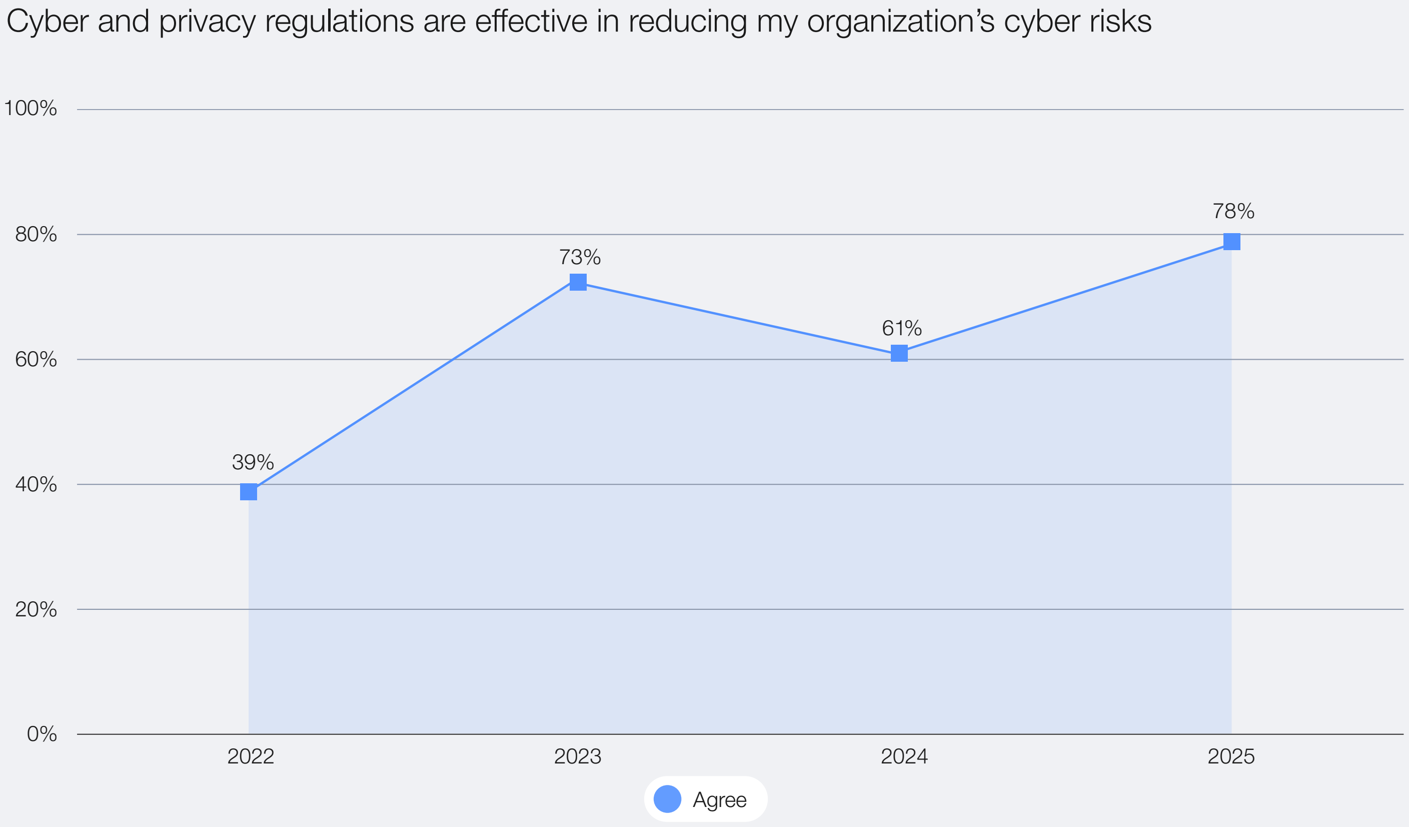
However, though the model we implemented for the Olympic Games worked well and could be reused for similar use cases, there are two takeaways. First, this model was designed mainly to focus on certain essential entities and cannot be scaled up for all of society. Second, geopolitical tensions are rising, and so will the number and complexity of cyberattacks. Henceforth, it will be essential to keep pushing for more cyber prevention and strive towards collective cyber resilience. Though regulations and government are part of the solution, they cannot solve all cybersecurity issues. Everyone has a role to play to overcome these challenges, and it is therefore necessary to collectively identify new ways to leverage awareness and increase engagement across society.

Vincent Strubel
Director General, National Cybersecurity Agency of France

Reinforcing ecosystem resilience through regulation

Regulation serves as an important driver of cyber resilience, with 78% of CISOs and 87% of CEOs surveyed identifying the primary motivations for implementing new cyber-related regulations to be improving their organization's security posture and mitigating cyber risks. In dealing with systemic ecosystem risk, CISOs affirm the relevance of regulations in imposing minimum requirements on the cybersecurity of organizations, which helps reduce risk and increase customer trust. At the same time, two-thirds of respondents to the GCO survey indicated that proliferation of cyber regulations worldwide adds significant complexity, with businesses having to navigate an increasingly fragmented landscape of regional and global compliance requirements.

FIGURE 11 **The effect of regulation in reducing organizational cyber risk**



In the European Union, the NIS2 Directive significantly raises the bar for cybersecurity standards, requiring enhanced incident reporting, stricter supply chain oversight and increased accountability for boards of directors. Across the Atlantic, the United States is enforcing CISA's Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), mandating the prompt disclosure of cyber incidents. In the Asia–Pacific region, countries such as Japan and Singapore are strengthening their cyber laws, with Japan's Act on the Protection of Personal Information (APPI) and Singapore's Cybersecurity Act reinforcing compliance for critical infrastructure operators. Additionally, initiatives such as the Digital Operational Resilience Act (DORA), the EU's General Data Protection Regulation (GDPR), Nigeria's Data Protection Regulation (NDPR) and Brazil's General Data Protection Law (LGPD) extend regulatory scrutiny across sectors and borders.

While these legal frameworks mandate important cybersecurity practices, they also introduce challenges, such as managing overlapping requirements, achieving compliance in multiple jurisdictions and addressing varied enforcement timelines. The line between regulated and unregulated sectors further complicates resilience, as industries with weaker oversight become conduits for attacks on more fortified entities. Organizations must adopt holistic risk-management approaches, align cybersecurity with governance structures and promote cross-border collaboration to thrive in this increasingly regulated landscape.

69%

of GCO survey respondents find regulations too complex or too numerous, or have difficulty verifying whether third-party suppliers are compliant.

The GCO survey has shown that organizations experience challenges in implementing existing cyber regulations, with more than 69% of respondents finding regulations too complex or too numerous, or experiencing difficulty verifying whether third-party suppliers are complying with the requirements. As regulatory pressure increases, there are concerns that the overwhelming number of updated or newly introduced regulations will lead to regulatory fatigue among companies and lose their desired effectiveness. While regulations set foundational standards and put cybersecurity on the agenda, there is a risk that the intricate “regulatory jigsaw puzzle” could detract from developing customized, risk-based strategies. Resilience requires not only meeting but exceeding regulatory demands. To address these challenges, there is an urgent need for public–private cooperation to enable global regulatory harmonization and alignment and ensure the applicability of cybersecurity standards throughout diverse regions. This would promote consistency while allowing for flexibility to adapt to emerging threats and technologies.

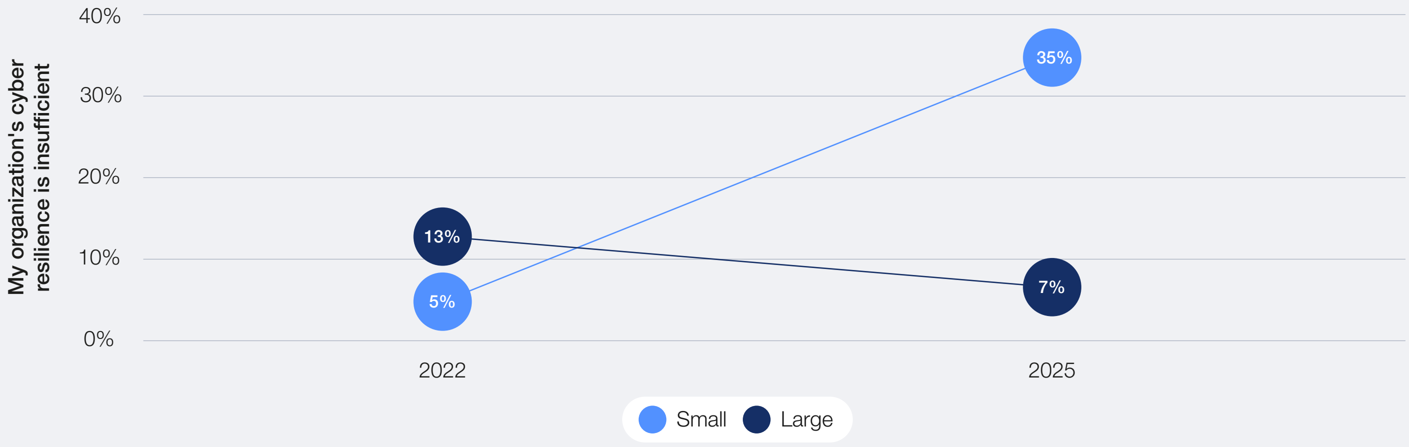
> **Today, Europe, like the rest of the world, is facing an increasingly complex threat landscape, coupled with rising geopolitical instability. Solidarity among like-minded partners in cybersecurity is needed more than ever. The cybersecurity legislation in the European Union, providing for a robust legal framework based on trust and cooperation, aims at creating convergence among international players – much like the aim of the World Economic Forum Annual Meeting on Cybersecurity.**
>
> Despina Spanou, Cybersecurity Coordinator, European Commission

Inequity as a driver of ecosystem risk

Systemic inequity in the global cybersecurity economy has worsened compared to the 2024 report. The *Global Cybersecurity Outlook 2025* finds that smaller organizations continue to feel the weight of this inequity, with 35% stating that their cyber resilience is insufficient.

FIGURE 12

Smaller organizations are struggling to ensure cyber resilience, while larger organizations show steady progress



At the other end of the spectrum, the number of large organizations reporting that their cyber resilience is insufficient has nearly halved. However, in an ecosystem that is becoming increasingly interconnected, the overall resilience of the ecosystem is often determined by its weakest links.

Larger, more resilient companies have a strong incentive to support smaller, less-capable organizations, thereby enhancing the resilience of the entire ecosystem. According to 71% of cyber leaders at the Annual Meeting on Cybersecurity 2024, small organizations have already reached a critical tipping point where they can no longer effectively secure themselves against the escalating complexity of cyber risks. This underscores the urgent need for collective action and treating cybersecurity as a strategic leadership imperative. Leadership engagement and oversight can prove to be a key differentiator in strengthening overall resilience. The survey reveals that in 62% of high-resilience organizations, board members received regular updates on recent cyber incidents, trends, vulnerabilities and risk predictions from internal or external third parties; this is in stark contrast to only 29% in low-resilience organizations.

CASE STUDY 3

Giving small organizations in Switzerland a leg-up with the help of public national infrastructure

> Three-quarters of Swiss companies make less than half a million CHF a year. The question is how can we meaningfully enable these companies to invest in security and how can we supply base infrastructure to them that is reasonably secure? We have many small- and medium-sized organizations that are insufficiently resourced. We conducted a pilot with a Swiss logistics company to help them manage their supply chain risks. Through collaboration with the independent National Test Institute for Cybersecurity (NTC), we are testing digital products for which there is a public but no immediate economic interest. We are currently boot-strapping a project where we review open-source software used by government agencies and we provide feedback to open-source developers to fix issues we found. We are additionally investing in capacity-building to help boards ask the right questions, because we believe we need to develop a culture among executives to think about resiliency and factor in the supply chain in their overall risk calculations.

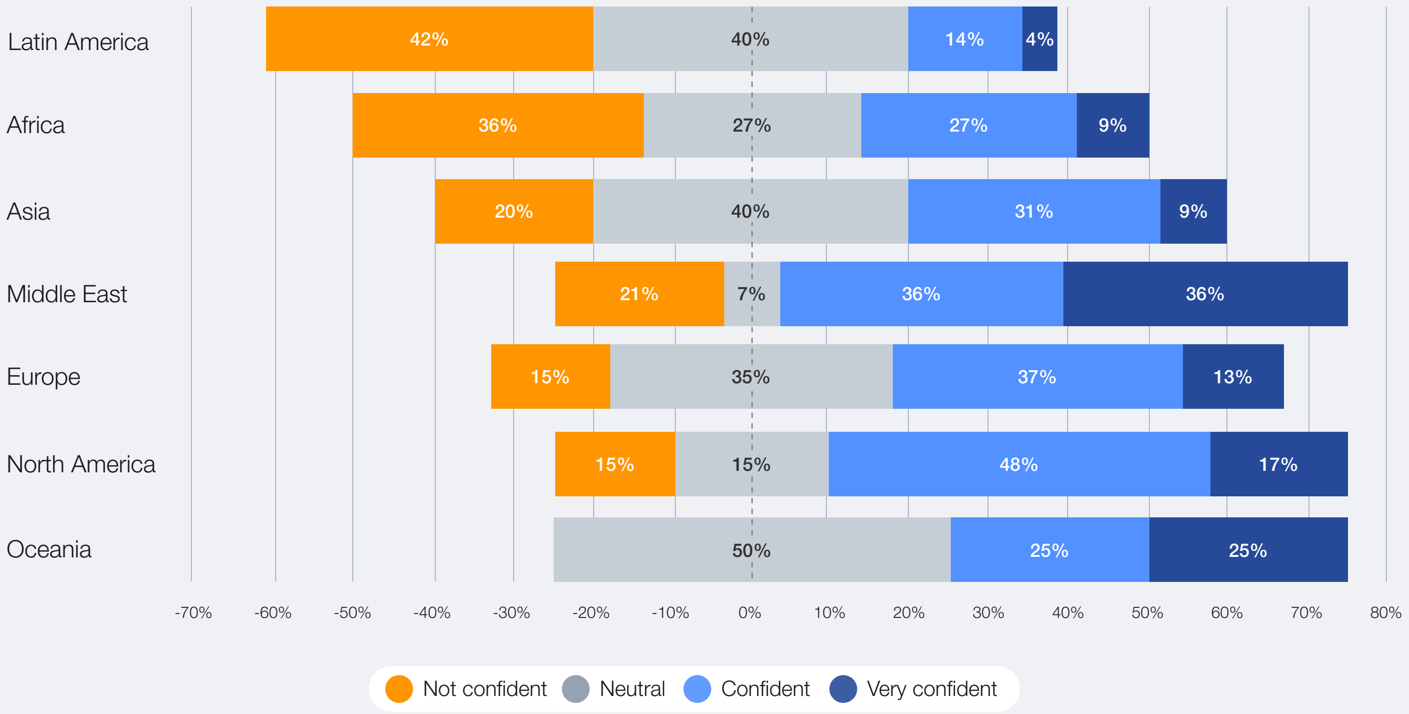
Florian Schütz
Director, National Centre for Cybersecurity (NCSC), Switzerland

Beyond the growing gap between large and small organizations, it is essential to take a more holistic view of cyber inequity. The term refers to the disparity between those with the resources and capabilities to secure their digital environments and those without. This gap spans several important areas, including access to infrastructure, financial resources, governance frameworks and the skilled employees necessary to build a robust cybersecurity posture. In light of this, it is important not only to consider the differences between large and small organizations but also to explore two additional perspectives.

1 **Developed vs. emerging economies:** The World Economic Forum's *Global Cybersecurity Outlook 2024* revealed that cyber inequity tends to mirror other global development indicators, with the lowest number of self-reported cyber-resilient organizations being in the Global South and the highest in the Global North. This disparity is also emphasized by the latest data. While in Europe and North America only 15% of organizations do not feel confident in their countries' preparedness to respond to major cyber incidents targeting critical infrastructure, in Africa and Latin America this figure goes up to 36% and 42% respectively. A successful attack on critical infrastructure such as the power grid or a seaport in less-prepared regions could trigger widespread disruption, resulting in serious consequences for economic stability and national resilience.

FIGURE 13 **Regional differences in cyber resilience**

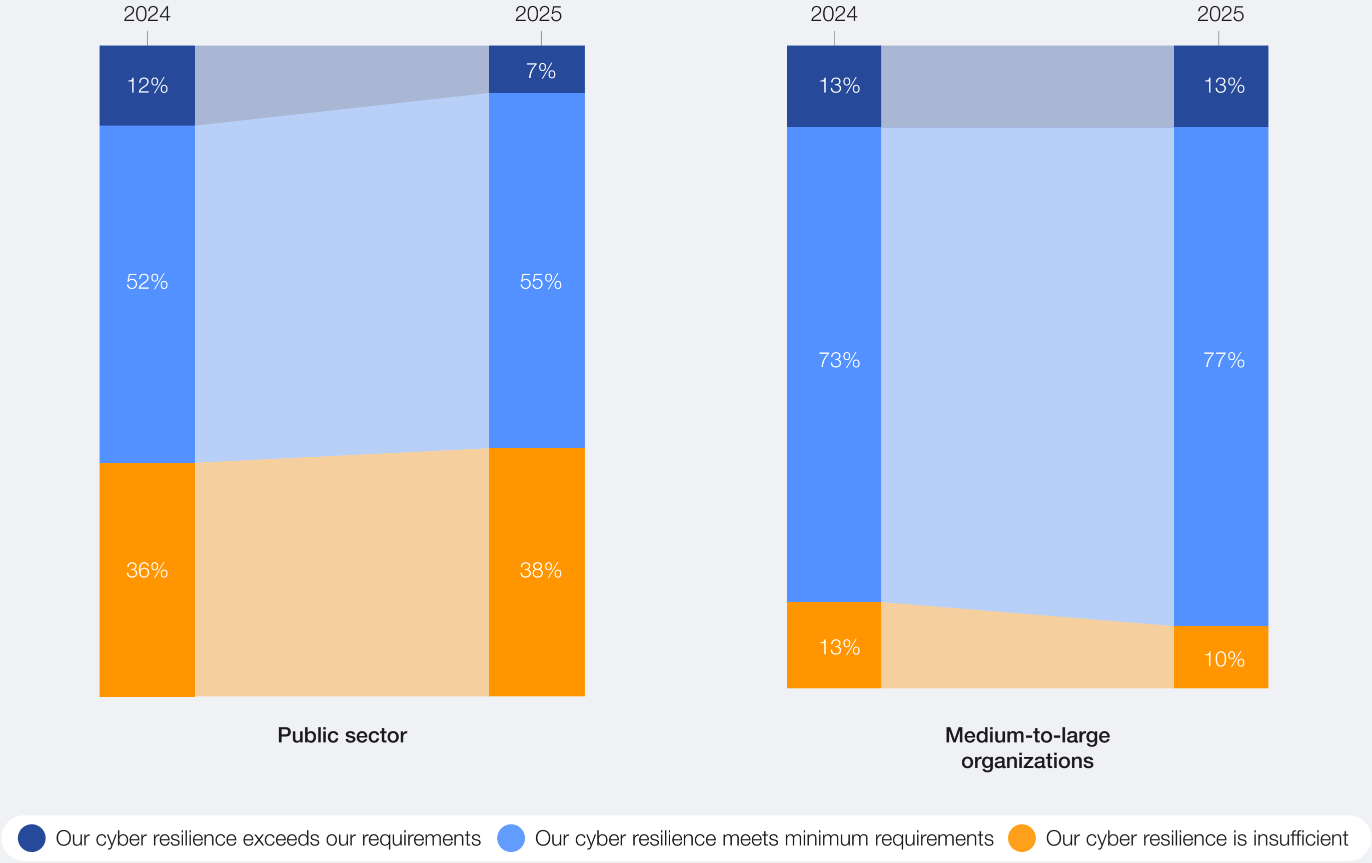
How confident are you that the country in which your organization is based is well prepared to respond to major cyber incidents targeting critical infrastructure?



2 **Sectoral disparities:** When observing the security posture of businesses by sector, finance is the most advanced. This is largely due to the environment within which the sector operates. A combination of industry- and geography-focused regulations in the US and Europe, for example, drives cybersecurity advances through compliance obligations. In contrast, sectors such as manufacturing are still in the early stages of building a culture of cyber resilience. Resource constraints and available infrastructure further exacerbate these disparities, particularly in the public sector. The survey findings reveal that 38% of public-sector respondents perceive their resilience to be inadequate, compared to only 10% of medium-to-large organizations in the private sector.

FIGURE 14 **Public-sector vs. medium-to-large organization confidence about cyber resilience**

How do you feel about your organization's ability to be cyber resilient?



These dimensions of cyber inequity can also increase workforce-related challenges. Today's global demand for cybersecurity professionals exceeds supply. While large organizations, particularly those in developed markets, are naturally well positioned to harness these scarce resources, the workforce inequity extends beyond organizational and geographic disparities. Certain sectors – such as education, government and healthcare as well as small and medium-sized enterprises (SMEs) – are disproportionately affected by the gap of cybersecurity professionals.

> **Driven by national institutions and centres of excellence, Brazil is making significant strides in cybersecurity maturity. To address cyber inequity, enhance resilience and secure national infrastructure, the recently established National Cybersecurity Committee (CNCiber) is developing a new National Cybersecurity Strategy (E-Ciber) and proposing a national governance body. The E-Ciber will prioritize resilience for essential services, foster intersectoral collaboration and invest in cybersecurity education, while the governance body will coordinate, regulate and monitor national cybersecurity efforts, ensuring a better security posture in the cyber ecosystem.**
>
> Andre Luiz Bandiera Molina, Secretary of Information and Cyber Security of Brazil

CASE STUDY 4

How KPMG helped the FCDO create a safer, more accessible digital world

Between 2020 and 2024, KPMG supported the UK's largest overseas cyber capacity-building project in history. The UK's Foreign, Commonwealth and Development Office (FCDO) wanted to improve digital access and safety in five key developing markets. One pillar was focused on helping those markets to become more cyber-savvy, safe and resilient.

The programme involved a consortium of 21 suppliers across six countries. Coordinated by KPMG, they worked together to address the significant impacts of cyber threats in developing countries and preventing harm to citizens and businesses. Judges were trained to help improve cyber prosecutions, small businesses' defences were bolstered and a national cybersecurity school curriculum was created. Government staff were trained in cybersecurity and a new Data Protection Commissioner Office was established. In Brazil, the materials reached up to 120 million people. One project in Nigeria reached more than 10% of the population.

The programme delivered outsized, sustainable impacts, and the blueprint it created is now being considered for other markets – including Ukraine and India.

2.4 The state of cyber resilience

Cyber resilience – defined as an organization's ability to minimize the impact of significant cyber incidents on its primary goals and objectives – demands continuous vigilance and planning.[41] Accepting that 100% security is unattainable, organizations must develop adaptable strategies that contribute to uplifting not only their own organizational resilience but also that of the wider ecosystem on which their own resilience depends.

The organizational response to the cyberthreat landscape

63%

of organizations cited complex and evolving threat landscape as their greatest challenge to becoming cyber resilient.

Some 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. Organizations must continually prepare to respond to cyberthreats, with the basics of cyber hygiene – including a continued focus on foundational practices and a process to manage vulnerabilities – not being neglected amid rapid technological adoption and change.

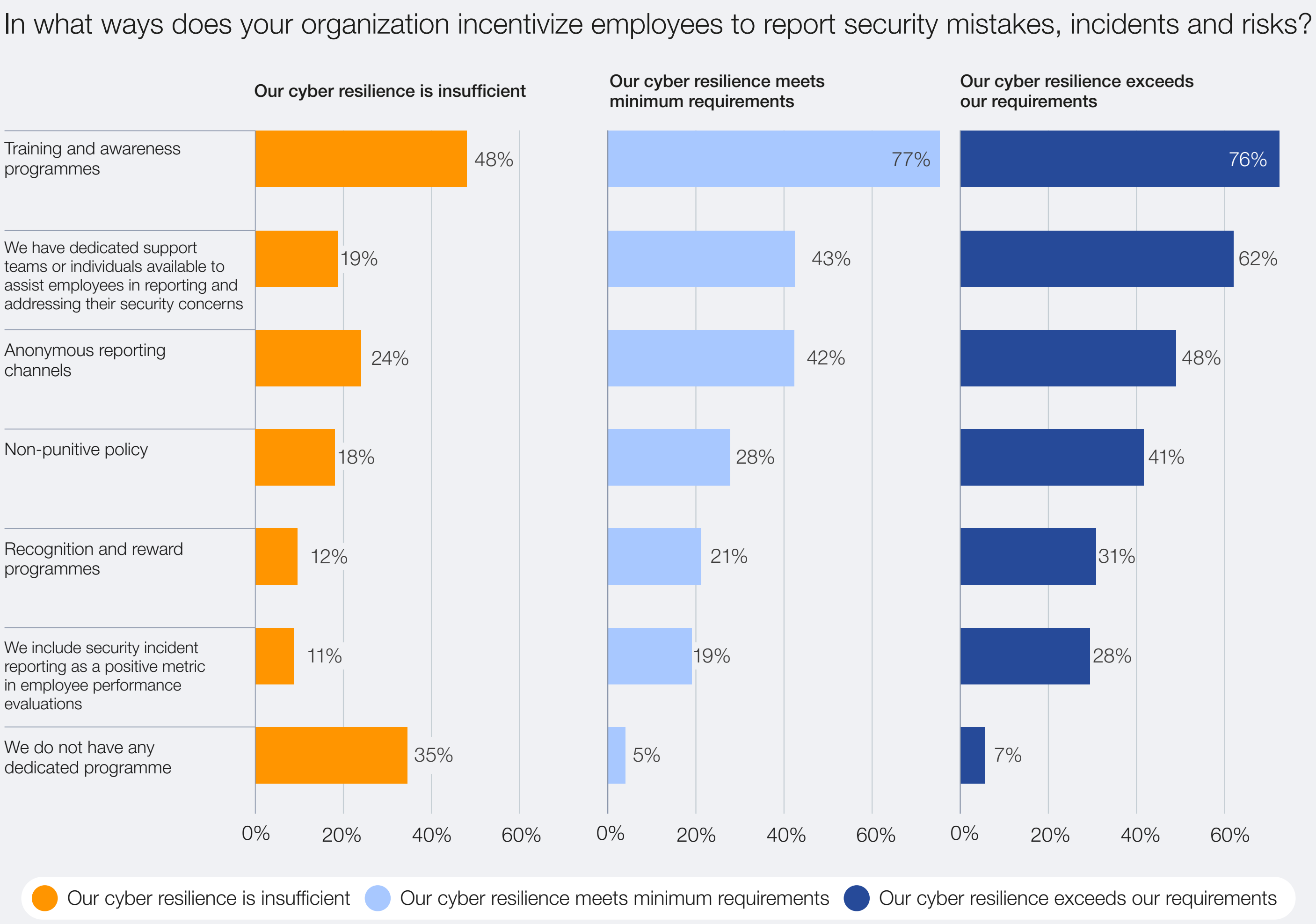
Public–private partnerships and collaboration have been shown to be of increasing value in addressing the complexity of modern cyberthreats. Of the surveyed organizations, 50% rank information-sharing and threat intelligence as the most effective international cooperation measure – for example, through computer emergency response teams (CERTs) or information-sharing and analysis centres (ISACs). As cybercrime becomes more sophisticated and borderless, defenders are embracing international collaboration through an ecosystem-based approach to allow for collective defence against sophisticated criminal groups. While information- and intelligence-sharing are critical, leaders at the 2024 Annual Meeting on Cybersecurity concluded that such efforts are still fragmented and siloed, hindering effective action.

Incident response and management

The capacity of organizations to orchestrate a timely and effective response to cyber incidents is being tested by the increasingly complex nature of cyberthreats faced today.

Essential to effective incident response is a security culture that emphasizes openness and transparency. High-resilience organizations establish incentives for incident reporting through various supportive measures: 76% provide cyber training and awareness, 62% have supporting teams to assist in reporting and 48% operate anonymous reporting channels. Such an environment nurtures collaboration and a collective defence mindset, which is critical for addressing sophisticated and complex threats.

FIGURE 15 | **Incentives to encourage the reporting of cybersecurity threats and incidents**



CASE STUDY 5

Building skill sets for cybersecurity incident response in Indian cooperative banks

> The Indian cooperative banking system plays a vital role by offering a community-focused inclusive approach to banking, particularly in rural and agricultural communities. These banks use the upstream services from commercial banks for their customers, as they are cost-effective for a low volume of transactions, and doing so is less time-consuming and easy to implement – thus driving financial inclusion, promoting economic stability and supporting grassroots-level growth.
>
> Due to the growing sophistication of cyberthreats, the resource-starved cooperative banks face significant cybersecurity challenges. Lack of trained staff and reduced confidence in carrying out incident response makes them vulnerable to cyberattacks. To level the cyber field, CERT India introduced a structured programme, implemented over eight months with 40 identified cooperative banks, comprising cyber drills for bank officers to build incident-management capabilities. The programme provided an integral relationship between knowledge and cognitive process by encouraging critical thinking for problem solving in incident management.
>
> To evaluate the cumulative resiliency of these banks, the cyber drills were mapped to the four pillars of resilience: anticipate, withstand, recover and evolve. Weighted summation of the pillars was calculated showing significant resiliency improvement pre and post programme.
>
> **Sanjay Bahl**
> **Director-General, Indian Computer Emergency Response Team**

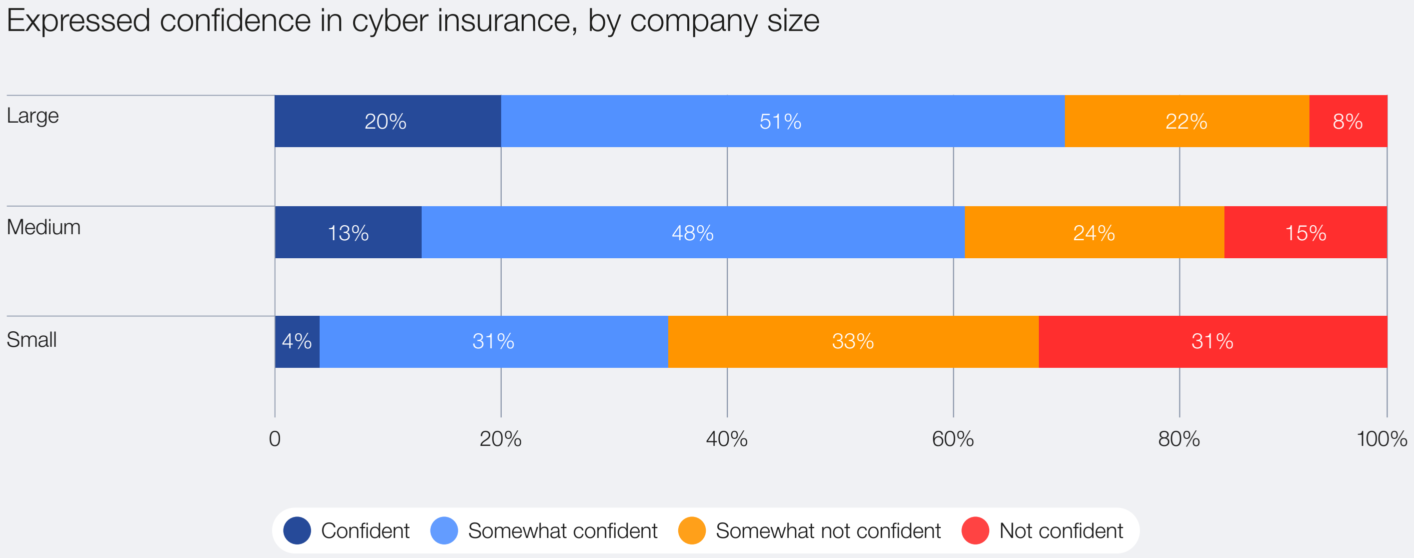
Formal processes for handling cyber incidents have become a mainstay within organizations, with the GCO survey showing only 13% of surveyed organizations lack any such cyber-incident management capability. The most common features include cyber-incident response playbooks, crisis exercises and internal response abilities. Interviewees for this report stress that playbooks are crucial for effective threat management, advocating for tailored escalation paths according to the incident type and creating structured responses that factor in the breach's scope and impact.

Cyber insurance

Insurance is one important tool among the portfolio of risk-management strategies that organizations can employ to address risk, with insurance offerings to cover the impacts from cyber events becoming more mature in recent years. Industry experts estimate that the size of the global market for cyber insurance will grow from $14 billion in 2023 to $29 billion in 2027.[42] From the survey, it appears that having some form of insurance aids organizations to become more cyber resilient: among organizations classed as highly resilient, only 7% claimed to not have cyber insurance.

However, cyber insurance appears to benefit larger organizations more than small organizations, likely because they are better able to afford it. In the survey, 71% of large organizations expressed confidence in their cyber insurance to adequately cover potential losses due to cyber events, as opposed to only 35% of small organizations. This again amplifies cyber inequity, with smaller organizations being more exposed to risk.

FIGURE 16 **How cyber insurance confidence varies by organization size**



Complexity at the intersection of IT and OT

The security of the OT environment is an important area affected by the growing complexity in cyberspace. Though the convergence of IT and OT is a recognized dynamic, they remain distinct in their characteristics and the attention they require, with IT and OT teams traditionally working at different ends of the technology stack and data flow. They tend to approach, prioritize and govern cybersecurity differently. Lack of collaboration on a formal IT/OT convergence strategy hinders the secure digitalization of industrial environments.[43] Strategic planning for OT security typically takes place over long timelines, is often dependent on highly specialized suppliers and therefore does not have the same agility to adapt within the typical investment lifespan of production systems, as is common in IT systems. Organizational cyber resilience is the sum total of resiliency of all parts, which means that IT and OT can no longer be treated in isolation as holistic risk-management strategies are designed.

CASE STUDY 6

Schneider Electric's comprehensive approach to operational technology (OT) cybersecurity

Schneider Electric's products are integral to several vital infrastructure providers such as power plants, solar farms, critical buildings and data centres that operate in increasingly connected environments. Given the importance of these sectors to national and global resilience, cybersecurity is of the utmost priority.

Consequently, Schneider Electric uses "security by design" with secure development life-cycle principles and independent penetration testing for its products while emphasizing securing its factories for manufacturing.

Further, Schneider Electric embraces "security by operations", including continuous monitoring and real-time threat detection, which is central to protecting operational environments through the entire value chain, with clarified responsibilities to maintain robust security measures at every stage. It also prioritizes regular security assessments and updates to ensure its systems remain resilient against evolving cyber threats.

A key initiative, developed in partnership with BitSight, involves scanning the internet and detecting exposed unsecured OT protocols that are "open doors" to critical environments and proactively mitigating associated risks in collaboration with customers and authorities.

Through these efforts, Schneider Electric demonstrates a commitment to working collaboratively with all relevant stakeholders and leveraging advanced security technologies to create a more secure and reliable operational environment for its customers.

The cyber skills gap

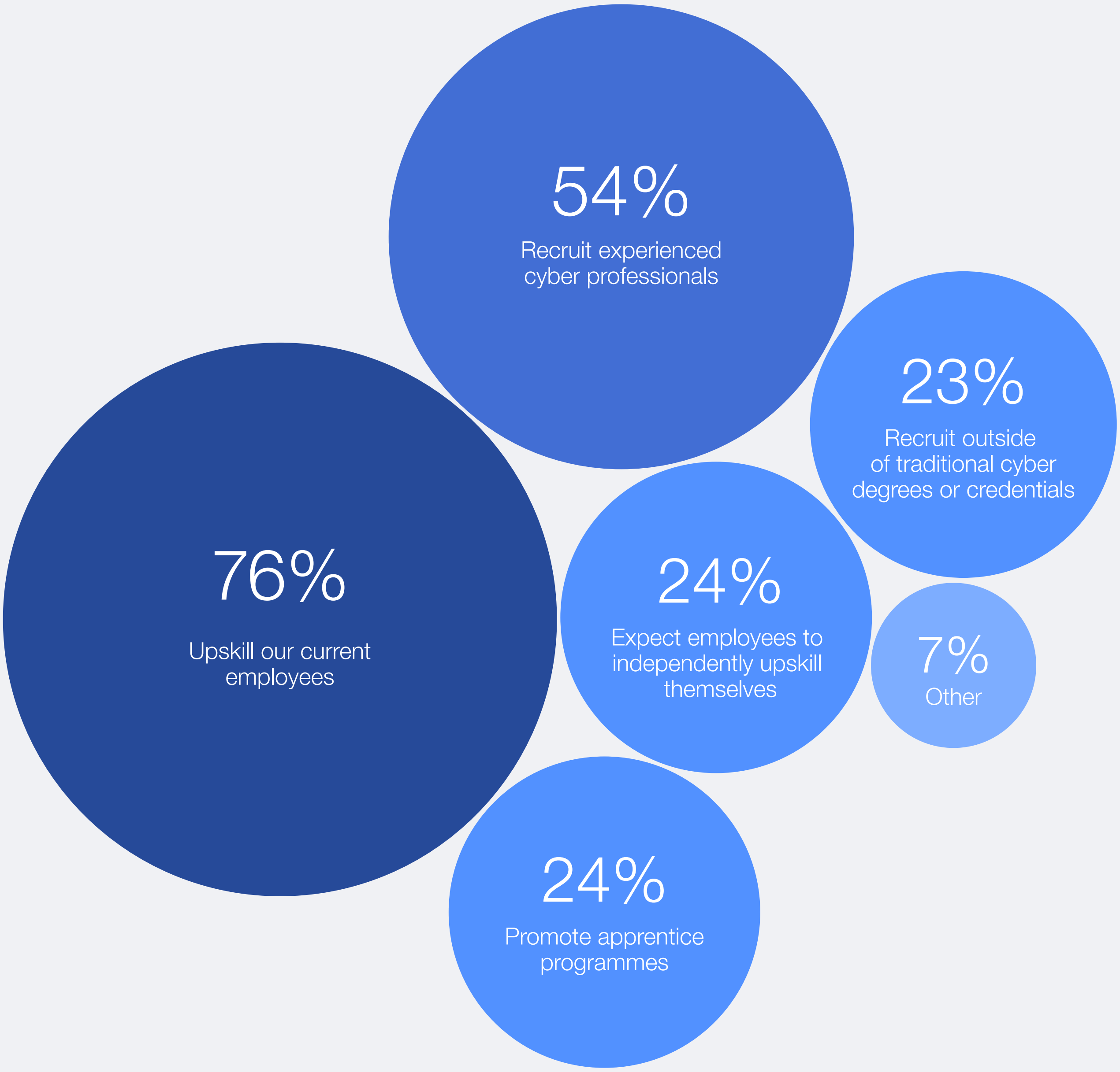
The cyber skills gap continues to be a key challenge to organizations becoming more resilient. The cybersecurity sector is grappling with a significant workforce shortage, with estimates of the shortfall ranging from 2.8 million to 4.8 million cybersecurity professionals. The acute scarcity of cybersecurity talent exacerbates the risk landscape, leaving more than two-thirds of organizations vulnerable to sophisticated cyberattacks and breaches due to a lack of critical skills.[44]

According to the GCO survey, while 39% of organizations cite skills shortages as an important barrier to resilience, only 14% report having the necessary talent to meet cybersecurity objectives.

The skills gap widened by 8% from 2024 to 2025, predominantly affecting the public sector, in which 49% of organizations indicated they do not have the workforce to meet their cybersecurity objectives, a 33% increase on 2024.

Skills in operating AI and defending against it are becoming increasingly important for the next-generation cybersecurity workforce. While AI will not replace the cybersecurity workforce, it will be a complementary capability. This presents an opportunity to begin closing the cyber skills gap, not only with increased automation but also with a workforce proficient in harnessing AI to drive positive outcomes for cybersecurity.

FIGURE 17 **How organizations are addressing the cyber skills gap**



Some 91% of participants in a focus group at the Annual Meeting on Cybersecurity 2024 concurred that AI would generate novel roles in cybersecurity, enhancing areas such as incident response. Yet 67% noted a shortfall in investments in AI skills within their organizations, signalling a disconnect between current training and the evolving demands. Companies must therefore commit to equipping their workforce with the necessary AI competencies, ensuring that educational curricula are continually updated to mirror the dynamic cyberthreat landscape and emerging technologies.

An important aspect of how AI can optimize human capital and training for the purposes of cybersecurity is its capacity to translate complex cyberthreat data into natural language. This can help reduce the dependence on technically astute analysts to understand the environment. According to a recent Institute for Security and Technology (IST) report: "[a]cross the board, LLMs have simplified data comprehension for all security personnel, though their impact has been particularly transformative for Tier 1 Security Operations Center (SOC) analysts during case investigations by reducing the time needed to accurately identify malicious intent".[45]

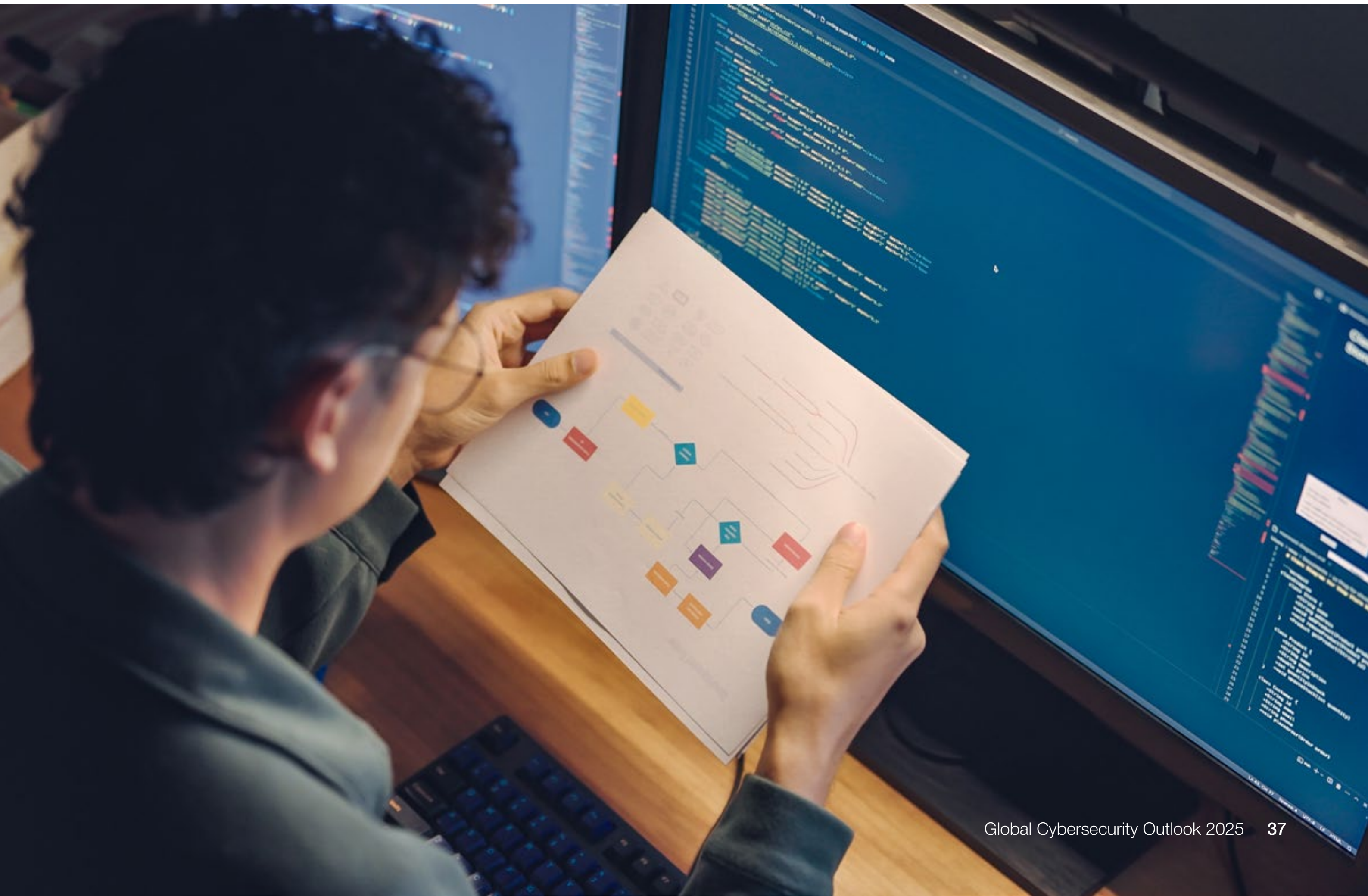
In addressing the evolving demands of cybersecurity, only 23% of organizations in 2025 are looking beyond traditional cyber qualifications to recruit talent from non-traditional backgrounds, such as communication, law and finance. As cybersecurity becomes more complex but also more important to the business, the need for professionals who can bridge the gap between technical details and business impact is ever more critical. Effective storytelling to translate complex cybersecurity issues into everyday language is an important part of engaging stakeholders and guiding informed decision-making.

BOX 2

Strategic Cybersecurity Talent Framework

In April 2024, the World Economic Forum released the *Strategic Cybersecurity Talent Framework*, featuring achievable approaches intended to help organizations build sustainable talent pipelines. This outlines how to attract more talent into cybersecurity by improving the understanding of what cybersecurity professionals do, removing barriers to entry and increasing diversity in the workforce. It also discusses how to equip students and professionals with essential skills for a career in the field, and suggests a rethink of recruitment practices to address challenges such as unrealistic and demanding requirements in job descriptions and misalignment between hiring managers and human resources (HR) departments. Finally, it investigates the promotion of retention strategies that generate a culture to inspire and motivate employees.

As the digital landscape continues to evolve, mapping the framework against emerging technologies, such as GenAI, becomes essential in ensuring its relevance and adaptability.



In addition to recruiting, retention is also important. A 2023 report by Gartner estimated that by 2025, almost half of cyber leaders would have moved into new jobs, while 25% would have transitioned into completely different roles because of work stressors.[46] Burnout poses a significant retention challenge, given the unpredictability and relentless demands of the role. Research from Proofpoint shows that 66% of CISOs believe that organizations place excessive expectations on them, with more than half having experienced or witnessed burnout in the previous 12 months.[47] The cybersecurity sector must prioritize the well-being of its workforce, incorporating considerations of human impact into its decision-making processes to avoid burnout and help talent retention.

> **Technology is pervasive in all of our lives, and in the era of AI, the threat surface is expanding rapidly and creating even more need for advanced cybersecurity. It's critical we help close the growing cyber skills gap with a focus on training, reskilling, recruiting and retaining cybersecurity talent. The technology sector has an important role to play, and Cisco is proud of our longstanding skill-to-jobs programme, Cisco Networking Academy, which works to close this gap.**
>
> Chuck Robbins, Chair and Chief Executive Officer, Cisco

> **Closing the cybersecurity skills gap is essential for safeguarding enterprises and addressing global workforce shortages. Programmes like Cyber Girls, Africa's biggest female-focused cybersecurity training programme, not only equip women with critical cybersecurity expertise but also empower them to enhance their own well-being and economic prospects. Investing in such programmes is a vital step towards building a more secure and inclusive digital future.**
>
> Confidence Staveley, Founder, CyberSafe Foundation

BOX 3

The evolution of the CISO role

In light of the growing complexity in cyberspace and the proliferation of regulations demanding the board's attention to cyber risks, organizational leadership is increasingly looking to the CISO to understand the cyber risks facing the organization. A poll of CISOs at the 2024 Annual Meeting on Cybersecurity revealed that 60% discuss the cybersecurity posture of the organization three to four times every year with the board. This requires CISOs not only to grasp the technical details of security but also to translate technical risk into business impact, articulating cyber risks in terms of financial loss, regulatory impact and customer trust and providing the board and C-suite with clear insights into how cybersecurity investments safeguard the business's bottom line and long-term viability.

Effective CISOs frame cyberthreats as business risks rather than purely technical challenges. By contextualizing cyber incidents in terms of business continuity, reputation and financial impact, they enable CEOs and boards to view cybersecurity as part of the broader risk landscape. For instance, certain CISOs now quantify cyber risk by its effects on market share, brand trust, safety and regulatory compliance, showing how cyber incidents can ripple throughout an organization, affecting shareholder value, market share, competitive positioning for mergers and acquisitions and customer trust. This approach is driving CEOs to advocate for a cyber-resilience strategy that not only addresses immediate threats but also supports long-term business stability.

Considering the importance of the CISO role, there is an increasing amount of focus on its reporting line within the organization, because this is an indicator of the influence the position wields in helping determine overall business strategy. Nearly 24% of CISOs polled at the Annual Meeting on Cybersecurity had a direct reporting line to the CEO, which confirms the growing importance of this role.

3

Navigating complexity in cyberspace

Leaders must prioritize cybersecurity as a strategic investment to ensure resilience amid emerging new threats.

> **The 2022 cyberattacks on Costa Rica served as a wake-up call, underscoring the need for a fundamental shift in recognizing cybersecurity as a critical investment for the future rather than a mere expense. The impact of these cyberattacks not only heightened awareness about cybersecurity issues but also drove transformation within institutions, making cybersecurity a core topic even at the household level. Through this journey, we have recognized the need to strengthen our ecosystems by collaborating with our neighbours to enhance resilience not only in Costa Rica but also across the region.**
>
> Paula Bogantes Zamora, Minister of Science, Innovation, Technology and Telecommunications of Costa Rica

The *Global Cybersecurity Outlook 2025* highlights the growing complexity in cyberspace, driven by factors such as geopolitical uncertainty and the increasing sophistication of cybercriminals – elements that often lie outside the direct control of organizational leaders. Nevertheless, it is crucial for leadership to understand the cumulative impacts of this complexity on both organizational and national cybersecurity postures.

Addressing this deep-rooted complexity is no mean feat. It requires out-of-the-box thinking, almost always needing an economic argument to highlight the price of inaction on cybersecurity.

3.1 Introducing the economics of cybersecurity

Since past cyberattacks have highlighted the intrinsic link with the broader economic context – most notably in cases where attacks have caused measurable damage to economies as a whole – the financial drivers and consequences of cyber incidents are increasingly capturing the attention of leaders in both the private and public sectors The rise of organized cybercrime, large-scale attacks targeting critical infrastructure and the fast pace of technological adoption affecting social and economic development highlight the far-reaching economic impacts of cybersecurity.

Another critical aspect is to understand the erosion of economic value due to cybercrime. With minimal operational costs and potentially high returns, cybercrime has become a highly profitable venture for attackers. The US Federal Bureau of Investigation (FBI) estimates that losses resulting from cybercrime exceeded $12.5 billion in 2023.[48] As cybercriminals become more organized and innovative, many businesses are turning to cyber insurance to mitigate the financial impact of cyberattacks. However, with the increasing frequency of cybercrime, insurers are adjusting premiums and coverage terms, making it more expensive for businesses to secure adequate protection.

All of these factors point to the need for leaders to quantify cyber risks and their economic impacts to align investments with core business objectives, while leaders who have the resources and means to help those who do not may need to step up to ensure a whole-of-system approach.

One of the core tenets of cyber economics is the balancing act between investing in cybersecurity and managing competing business priorities. The rising complexity of the cyber landscape means that cyber risk is touching more parts of organizations, and successful leaders must correspondingly navigate a risk landscape in the same way as they do a market environment. Even though more than 60% of CEOs and CISOs surveyed report that cyber-risk management is integrated into enterprise risk management in their organizations, many still struggle to accurately assess the level of required investment. In fact, today, fewer than half of CEOs believe their organizations invest enough in cybersecurity.

While proactive security measures – including multifactor authentication, firewalls and security-awareness training – can be costly, such expenses are negligible compared to the financial consequences of a cyberattack. However, in cash-strapped SMEs, such costs can be challenging unless compelling incentives can be introduced. In attempting to identify incentives, it is interesting to draw parallels with global efforts to combat a crisis in the physical realm – the climate crisis. Across the world, countries are trying to create incentives to push citizens in the direction of renewables, with significant subsidies being offered to help drive the movement towards rooftop solar or heat pumps, for example. To drive affirmative action and boost cyber resilience through the uptake of proactive security measures, it seems reasonable to demand similar incentives aimed at SMEs from governments.

One of the critical barriers to adequate investment in cybersecurity is the inability to effectively quantify cyber risk due to the constantly evolving threat landscape as well as the complexity of estimating the potential impact of cyber incidents. Yet being able to articulate cyber risk in financial terms is essential for organizations to allocate resources effectively and build resilience.

The economic dimension of cybersecurity is also reflected in the demand for a cyber workforce. The emergence of a rapidly growing cybersecurity job market offers individuals the opportunity to build long-term and financially rewarding careers. New employment opportunities not only help boost individual livelihoods but also contribute to overall economic development in industries and geographies.

While cyber economics is a broad concept that needs greater exploration, the case for building cyber resilience on the back of sound economic arguments is compelling – one, in fact, that leaders can no longer afford to ignore. With committed leadership, smart investment and a culture of security, organizations can build resilience that permeates the entire organization.

Conclusion

Escalating complexities in cyberspace challenge ecosystem cyber resilience and expose gaps in preparedness.

The increasing complexity of cyberspace presents a profound challenge to achieving cyber resilience, exacerbating inequities that leave less-resourced organizations vulnerable. Geopolitical tensions are prompting organizations to re-evaluate their strategies, balancing security concerns with global operations. Such tensions often drive targeted attacks, as state-sponsored actors exploit vulnerabilities for espionage and disruption. This dynamic landscape requires adaptive strategies that account for shifting global risks and supply chain dependencies.

At the same time, the growing sophistication of cybercriminals remains a persistent challenge. AI-enhanced tactics, Ransomware-as-a-Service and advanced social engineering methods enable threat actors to outpace traditional defences. Addressing these evolving threats demands not only advanced technological solutions but also cross-sector collaboration and knowledge-sharing.

Despite these obstacles, there is cause for cautious optimism. Organizations that embrace proactive risk management, prioritize collaborative approaches across ecosystems and invest in scalable, equitable solutions can help reduce disparities. Addressing systemic vulnerabilities – such as supply chain dependencies and skill shortages – will be essential to promoting a resilient digital ecosystem.

Ultimately, overcoming today's challenges requires not just technological innovation but a shift in perspective. Cyber resilience must be recognized as a collective responsibility, with organizations of all sizes working together to fortify the interconnected networks that underpin the digital economy. Further, there is a need for decisive leadership action to prioritize cybersecurity among and between organizations; beyond technical indicators, robust criteria rooted in the economic implications of cyber insecurity will be required. A united leadership team, in which business and cyber leaders see eye to eye on the cyber risks facing the organization, is critical to navigating growing cyber complexity.

Appendix: Methodology

The *Global Cybersecurity Outlook* (GCO) survey was the primary dataset used as the foundational research for this report, with 24 questions for all respondents (plus five questions specifically for CISO respondents) and an additional seven demographic questions. The survey was launched on 2 September 2024 and ran until 11 October 2024. The World Economic Forum received responses from 409 survey participants from 57 countries. Once the dataset was normalized using the seven demographic questions to determine the qualifications of participants, the dataset was left with 321 qualified participants. Each of the 321 participants fully completed the survey.

To provide additional qualitative data, 43 one-on-one interviews were conducted with C-suite executives, industry leaders and academics, asking adjacent or supplementary questions to probe further into the survey data collected.

In July 2024, a 90-minute workshop was held with 10 members of the Global Future Council on Cybersecurity, thought leaders from academia, government, international organizations, business and civil society, focused on themes to be featured in the GCO survey. Additionally, in October 2024, a 90-minute workshop was held with 20 executives from the World Economic Forum's Centre for Cybersecurity's CISO Community, focused on themes identified within this report. Additional quantitative data was collected in the form of a two-question poll posed to the attendees.

The Forum's Annual Meeting on Cybersecurity took place on 11–13 November 2024. Several sessions were held, and qualitative data was gathered from the 170-plus executives who attended the event. During the various sessions, quantitative data was gathered in a form of six poll questions for the audience.

Contributors

Lead authors

World Economic Forum

Akshay Joshi
Head, Centre for Cybersecurity

Giulia Moschetta
Initiatives Lead, Centre for Cybersecurity

Ellie Winslow
Coordinator, Centre for Cybersecurity

Fellows

Willem Buys
Project Fellow, Global Cybersecurity Outlook

Anna Herrmann
Project Fellow, Global Cybersecurity Outlook

Acknowledgements

World Economic Forum

Filipe Beato
Lead, Centre for Cybersecurity

Frédéric Calbert
Data Intelligence and Visualisation Lead,
Technology and Digital Services

Sean Doyle
Lead, Cybercrime Atlas Initiative,
Centre for Cybersecurity

Tal Goldstein
Head of Strategy,
Centre for Cybersecurity

Natasa Perucica
Project Lead, Centre for Cybersecurity

Accenture

Toms Bernhards Callahan
Research Specialist

Jacky Fox
Global Cyber Strategy Lead

Shachi Jain
Research Manager

Felicity March
EMEA Cyber Strategy Lead

Additional Acknowledgements

World Economic Forum

Joanna Bouckaert
Community Lead, Centre for Cybersecurity

Isabella Kaplan
Community Specialist,
Centre for Cybersecurity

Luna Rohland
Specialist, Cyber Resilience,
Centre for Cybersecurity

Apisada Suwansukroj
Lead, Programming and Communications,
Centre for Cybersecurity

Kesang Tashi Ukyab
Lead, Cyber Resilience, Electricity,
Centre for Cybersecurity

Natalia Umansky
Project Specialist, Cybercrime Atlas Initiative,
Centre for Cybersecurity

The World Economic Forum would like to thank the following individuals who shared their insights and knowledge in one-to-one interviews or community meetings.

Jad H. Abdulsalam
Ma'aden

Oz Alashe
CybSafe

Bushra AlBlooshi
Dubai Electronic Security Center

Hoda Al Khazimi
New York University Abu Dhabi

Yasser N. Alswailem
Saudi Telecom Company

Edward Amoroso
Tag Infosphere

Brad Arkin
Salesforce

Sachin Bansal
SecurityScorecard

Christophe Blassiau
Schneider Electric

Grant Bourzikas
Cloudflare

Niall Browne
Palo Alto Networks

Kris Burkhardt
Accenture

Sam Curry
Zscaler

Wallace Dalrymple
ETS

Michael Daniel
Cyber Threat Alliance

Mohammed Darwish Azad
Emirates NBD

Rob Dewar
Abertay University

Hazel Diez Castaño
Banco Santander

Dorit Dor
Check Point Software Technologies

Yusuf Ezzy
PG&E Corporation

Laurent Fabre
Banque Pictet

Sabrina Feng
London Stock Exchange Group

Sergio Fidalgo
BBVA

Janus Friis Bindslev
PensionDanmark

Daniel Frye
Hewlett Packard Enterprise

Richard Hale
Sony Group Corporation

Lars Idland
Equinor

Öykü Işık
IMD Business School

Stephanie Itimi
Seidea

Bill Jewell
US Chamber of Commerce

Steven Kelly
Institute for Security and Technology (IST)

Sigmund Kristiansen
Aker BP

Chua Kuan Seah
Cyber Security Agency of Singapore (CSA)

Kris Lovejoy
Kyndryl

Stefan Lueders
CERN

David Mabry
Gulfstream Aerospace Corporation

Klas Martinus Bendrik
DNV

Bec McKeown
Mind Science

Rishi Mehta
HCL Technologies

Eduardo Melendez Yudico
Grupo Salinas

Eiichiro Mitani
Mitsubishi Electronic Corporation

Paulo Moniz
EDP

Mark Orsi
Global Resilience Federation

Cezary Piekarski
Standard Chartered Bank

Robert Rodger
Admiral Insurance

Jason Ruger
Lenovo

Mehzad Sahar
Engro Corporation

Amir A. Samad
PETRONAS

Andreas Schmitt
Zurich Insurance

Ralf Schneider
Allianz

Florian Schütz
National Center for Cybersecurity,
Switzerland

Vikram Sharma
QuintessenceLabs

David Sherry
Princeton University

Bethany Singer-Baefsky
National Grid

Jennifer Tang
Institute for Security and Technology (IST)

Akhilesh Tuteja
KPMG

Amy Webb
New York University Stern School of Business

Friedrich Wetschnig
Flex

Kevin Winter
Deloitte Global Services

Annemarie Zielstra
KPMG

Additional contributors

The authors are grateful to KPMG's Fleur Boor-Zeeman, Kevin de Man and Mert Solen for their contributions to the *Global Cybersecurity Outlook 2025*.

The World Economic Forum would like to acknowledge the following organizations for their contributions to the *Global Cybersecurity Outlook 2025*: the Cyber Threat Alliance, the Global Cybersecurity Alliance, the Organization for American States, the Institute for Security and Technology and the Digi Americas Alliance.

The Forum also wishes to acknowledge contributions from Gretchen Bueermann, Kilian Hayat, Augustinus Mohn and Yanya Viskovich.

Production

Rose Chilvers
Designer, Studio Miko

Laurence Denmark
Creative Director, Studio Miko

Sophie Ebbage
Designer, Studio Miko

Alison Moore
Editor, Astra Content

Endnotes

1. The category of smallest organizations by annual revenue in the *Global cybersecurity outlook 2024* data is <$250 million; the category of medium is between $250 million and $5.5 billion; and the category of large is > $5.5 billion.
2. World Economic Forum. (2024, January). *Global cybersecurity outlook 2024.* https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf.
3. World Economic Forum. (2024, January 10). *Global risks report 2024*. https://www.weforum.org/publications/global-risks-report-2024/.
4. World Economic Forum. (2024, October). *Chief risk officers outlook: October 2024*. https://www.weforum.org/publications/chief-risk-officers-outlook-october-2024/#:~:text=Chief%20risk%20officers%20are%20most,anticipating%20volatile%20conditions%20has%20increased.
5. Ibid.
6. Fung, B. (2024). *We finally know what caused the global tech outage – and how much it cost*. CNN. https://edition.cnn.com/2024/07/24/tech/crowdstrike-outage-cost-cause/index.html.
7. Dor, D. (2024, October 22). *We must reduce complexity to ensure strong cybersecurity. Here's why.* World Economic Forum. https://www.weforum.org/stories/2024/10/strong-cybersecurity-reduce-complexity-risk-cyber/.
8. National Cyber Security Centre. (2024, January 24).*The near-term impact of AI on the cyber threat assessment.* https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat.
9. Europol. (2024, April 18). *International investigation disrupts phishing-as-a-service platform LabHost*. https://www.europol.europa.eu/media-press/newsroom/news/international-investigation-disrupts-phishing-service-platform-labhost.
10. United Nations Office on Drugs and Crime. (2023, September). *Casinos, cyber fraud, and trafficking in persons for forced criminality in Southeast Asia*. https://www.unodc.org/roseap/uploads/documents/Publications/2023/TiP_for_FC_Policy_Report.pdf.
11. BBC. (2024, August 23). *China scam run from Isle of Man.* https://www.bbc.com/news/articles/cz6x1ql1yelo.
12. Rogers, S. (2024, November 7). *International scammers steal over $1 trillion in 12 months in global state of scams report 2024*. Global Anti-Scam Alliance. https://www.gasa.org/post/global-state-of-scams-report-2024-1-trillion-stolen-in-12-months-gasa-feedzai.
13. BBC. (2024, June 14). *Hospitals cyber attack impacts 800 operations.* https://www.bbc.com/news/articles/cd11v377eywo.
14. United Nations Office on Drugs and Crime. (2024). *Transnational organized crime and the convergence of cyber-enabled fraud, underground banking and technological innovation in Southeast Asia: A shifting threat landscape.* https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf.
15. Accenture. (2024, July 30). *Beyond the illusion – unmasking the real threats of deepfakes*. https://www.accenture.com/us-en/blogs/security/beyond-illusion-unmasking-real-threats-deepfakes.
16. Antoniuk, D. (2024, April 23). *Russian hackers target 20 energy facilities in Ukraine amid intense missile strikes*. The Record by Recorded Future. https://therecord.media/russian-hackers-target-energy-facilities-ukraine.
17. Cybersecurity and Infrastructure Security Agency. (2024, February 23). *Top cyber actions for securing water systems*. https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems.
18. CNN. (2024, October 8). *American Water, the largest water utility in US, is targeted by a cyberattack.* https://edition.cnn.com/2024/10/08/business/american-water-cyberattack-hnk-intl/index.html.
19. Sebouai, L. (2024, July 12). AI, cyber-attacks and amateur experiments threaten to upend global biosecurity, WHO warns. *The Telegraph*. https://www.telegraph.co.uk/global-health/terror-and-security/ai-cyber-attacks-and-amateur-experiments-threaten-to-upend/.
20. World Health Organization. (2024). *Laboratory biosecurity guidance.* https://iris.who.int/bitstream/handle/10665/377754/9789240095113-eng.pdf?sequence=1.
21. Stawiska, Z. (2024, July 11). *Biosecurity guide warns of risks from AI, cyber-attacks, and amateur experiments.* Health Policy Watch. https://healthpolicy-watch.news/biosecurity-guide-warns-of-risks-from-ai-cyber-attacks-and-amateur-experiments/.
22. National Cybersecurity Center of Excellence (NCCoE). (n.d.). *Cybersecurity and privacy for genomic data*. National Institute of Standards and Technology (NIST). Retrieved December 5, 2024, from https://www.nccoe.nist.gov/projects/cybersecurity-and-privacy-genomic-data.
23. Sanger, D. E., et al. (2024, November 22). Emerging details of Chinese hack leave US officials increasingly concerned. *The New York Times* https://www.nytimes.com/2024/11/22/us/politics/chinese-hack-telecom-white-house.html.
24. Poirier, C. (2024, October). *Hacking the cosmos: Cybersecurity in space* (Cyber Reports 2024, 10). Center for Security Studies, ETH Zurich. https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/cyber-reports-2024-10-hacking-the-cosmos.pdf.
25. Astier, H., & Kirby, P. (2024, November 19). *Germany suspects sabotage over severed undersea cables in Baltic.* BBC News. https://www.bbc.com/news/articles/c9dl4vxw501o.

26. Schwab, K. (2024, September 24). *The Intelligent Age: A time for cooperation.* World Economic Forum. https://www.weforum.org/stories/2024/09/the-intelligent-age-a-time-of-cooperation/.

27. World Economic Forum. (forthcoming). *Artificial intelligence and cybersecurity: Balancing risks and rewards.*

28. KPMG. (2024). *KPMG 2024 CEO outlook.* https://kpmg.com/xx/en/our-insights/value-creation/kpmg-global-ceo-outlook-survey-2024.html.

29. Keller, J., & Nowakowski, J. (2024). *AI-powered patching: The future of automated vulnerability fixes*. Google Security Engineering Technical Report. https://research.google/pubs/ai-powered-patching-the-future-of-automated-vulnerability-fixes/.

30. Sells, J., & Turan, H. (2024, March 4). *Cloudflare launches AI assistant for security analytics*. Cloudflare. https://blog.cloudflare.com/security-analytics-ai-assistant/.

31. Reybango. (2023, November 10). *How AI can improve threat intelligence gathering and usage*. Microsoft Tech Community. https://techcommunity.microsoft.com/blog/educatordeveloperblog/how-ai-can-improve-threat-intelligence-gathering-and-usage/3975449.

32. Wang, Z., et al. (2024). *HoneyGPT: Breaking the trilemma in terminal honeypots with large language model*. arXiv preprint arXiv:2406.01882. https://arxiv.org/pdf/2406.01882.

33. Otal, H., & Canbaz, A.M. (2024, September 15). *LLM honeypot: Leveraging large language models as advanced interactive honeypot systems*. arXiv. https://arxiv.org/abs/2409.08234.

34. SPHINX Project. (2020, October 7). *SPHINX Toolkit components development: Artificial intelligence (AI) honeypot*. https://cyberwatching.eu.

35. US Department of the Treasury. (2024). *Statement on planning for opportunities and risks associated with quantum computing: G7 Cyber Expert Group*. https://home.treasury.gov/system/files/136/G7-CYBER-EXPERT-GROUP-STATEMENT-PLANNING-OPPORTUNITIES-RISKS-QUANTUM-COMPUTING.pdf.

36. World Economic Forum. (2024, January 17). *Quantum security for the financial sector: Informing global regulatory approaches*. https://www.weforum.org/publications/quantum-security-for-the-financial-sector-informing-global-regulatory-approaches/.

37. National Institute of Standards and Technology. (2024, August 13). *NIST releases first 3 finalized post-quantum encryption standards*. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

38. A software bill of materials (SBOM) is defined by NIST as a “formal record containing the details and supply chain relationships of various components used in building software”. Software developers and vendors often create products by assembling existing open-source and commercial software components. The SBOM enumerates these components in a product.

39. Turner, T. (2024, November 21). *SBOM requirements in the EU’s CRA (Cyber Resilience Act).* Fossa. Dependency Heaven. https://fossa.com/blog/sbom-requirements-cra-cyber-resilience-act/.

40. Microsoft. (2024). *Microsoft digital defense report 2024.* https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024.

41. Beato, F. (2024, November 11). *Unpacking cyber resilience.* World Economic Forum. https://www.weforum.org/publications/unpacking-cyber-resilience/.

42. MunichRE. (2024, February 4). *Cyber insurance: risks and trends 2024.* https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html.

43. World Economic Forum. (2024, April 29). *Building a culture of cyber resilience in manufacturing.* https://www.weforum.org/publications/building-culture-of-cyber-resilience-in-manufacturing/.

44. World Economic Forum. (2024, April). *Strategic cybersecurity talent framework.* https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf.

45. Institute for Security and Technology. (2024, October). *The implications of artificial intelligence in cybersecurity: Shifting the offense–defense balance*. https://securityandtechnology.org/wp-content/uploads/2024/10/The-Implications-of-Artificial-Intelligence-in-Cybersecurity.pdf.

46. Gartner. (2023, February 22). *Gartner predicts nearly half of cybersecurity leaders will change jobs by 2025* [Press release]. https://www.gartner.com/en/newsroom/press-releases/2023-02-22-gartner-predicts-nearly-half-of-cybersecurity-leaders-will-change-jobs-by-2025.

47. Proofpoint. (2024, May). *2024 Voice of the CISO. Global insights into CISO challenges, expectations and priorities.* https://nationalcioreview.com/wp-content/uploads/2024/06/pfpt-us-wp-voice-of-the-CISO-report.pdf.

48. FBI San Francisco. (2024, April 4). *FBI releases internet crime report.* FBI. https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-releases-internet-crime-report.

WORLD ECONOMIC FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org