# CYBERSECURITY FRONTIERS 2024:

## A Perspective on Securing the Future of Cyberspace

Insight Report

December 2024

GLOBAL
CYBERSECURITY
FORUM

Site

# Foreword

**Dr. Hesham Altaleb**
Saudi Information Technology Company (SITE), Chairman of the Knowledge Community: Future of Cybersecurity

As technological advancements accelerate at an unprecedented pace, cybersecurity has become an essential priority. This report intends to equip organizations with the knowledge to understand and navigate future cybersecurity opportunities and threats, whilst offering actionable recommendations aimed at strengthening defenses and harnessing the potential of emerging technologies.

By examining the dynamics of technological acceleration, international collaboration, and workforce transformations, the report identifies emerging trends and challenges set to shape the future cybersecurity landscape, providing foresight to help organizations remain proactive. Recognizing the complexity and urgency of cybersecurity challenges, the report also outlines strategic frameworks and practical guidelines designed to assist organizations in strengthening their cybersecurity posture, ensuring resilience and readiness against malicious actors.

This report is a result of numerous contributors' collective efforts and expertise, whose dedication and insights have been invaluable. It serves as an important resource for decision-makers, helping them to navigate the complexities of the cybersecurity landscape and supporting the creation of a secure and resilient digital future.

# Lead Authors

- **Bilal Baig** (Trend Micro)
- **Dikmen Edgu** (Axon Partners Group)
- **Álvaro García** (Axon Partners Group)
- **Dr. Almerindo Graziano** (Cyber Ranges)
- **Riku Valpas** (Fortinet)

# Contributors

- **Dr. Manar Alohaly,** Saudi Information Technology Company (SITE)
- **Dr. Bushra A. Alahmadi,** Saudi Information Technology Company (SITE)
- **Shoaib Yousuf,** Boston Consulting Group (BCG)
- **Radu Balanescu,** Boston Consulting Group (BCG)
- **Tin Pusic,** Boston Consulting Group (BCG)
- **Dan Bogdanov,** Cybernetica
- **Goran Safar,** Chainalysis
- **Thomas de Zoete,** Chainalysis
- **Dr. Andrey Bogdanov,** CYBERCRYPT
- **Dr. Mohammed Alenezi,** National Company of Telecommunications and Information Security (NTIS)
- **Sulaiman Almohsen,** National Company of Telecommunications and Information Security (NTIS)
- **Dr. Richard Weller,** Strategy&
- **Lucas Sy,** Strategy&
- **Piet Ramsl,** Strategy&
- **Abdulrahman Alosaimi,** International Business Machines (IBM)

# Knowledge Community: Future of Cybersecurity

The 'Future of Cybersecurity' is a Knowledge Community committed to exploring the potential opportunities and threats presented by the ever evolving Cyberspace and developing mechanisms to maximize the benefits and address the risks looming on the horizon, by bringing together a diverse array of expertise from various stakeholder groups.

The community welcomes leading technology companies, global cybersecurity organizations, cybersecurity research centers, reputable think tanks, academic institutions, and other stakeholders with a vested interest in exploring and acting upon the future of cybersecurity.

# Contents

## Disclaimer

This document has been published by the Global Cybersecurity Forum (GCF) in collaboration with Knowledge Partners as part of their efforts to promote thought leadership in cybersecurity. While GCF and the knowledge partners have made every effort to ensure the accuracy and reliability of the information provided, neither party assumes any responsibility for errors, omissions, or inconsistencies in the content, nor for any consequences arising from its use or interpretation. The content is provided for general information purposes and may be subject to change without prior notice at the discretion of GCF. This publication is protected by copyright law. No part of this report may be reproduced, distributed, or transmitted in any form or by any means—whether electronic or mechanical—without prior written permission from both GCF and the Knowledge Partners. All requests for such permissions should be directed to KC@GCForum.org.

Please consider the environment before printing this report

# 1. Executive Summary

**Are organizations well-prepared to tackle the cyber threats of the future?**

With technology advancing at an unprecedented pace, the attack surface for cyber threats has expanded – making it imperative to adopt comprehensive cybersecurity strategies. To secure and safeguard the digital realm against ever-evolving threats, it is crucial to understand and address its challenges. In this context, the Future of Cybersecurity Knowledge Community conducted an extensive survey, gathering insights from cybersecurity and emerging technology experts to understand the evolving threat landscape and the readiness of organizations.

## Technological Acceleration

Cybersecurity is considered as **competitive advantage**, but **few organizations are prepared for future challenges**

95%

**Consider cybersecurity as a competitive advantage**

86%

**Think organizations are not fully prepared for future challenges**

+90%

**Think that the threat landscape will change due to emerging technologies**

This report, informed by our survey, examines the evolution of cybersecurity through three critical dimensions: technological advancements, international collaboration, and workforce transformation. It provides actionable recommendations to fortify global cyber defenses and adapt to an increasingly interconnected world.

Emerging technologies like artificial intelligence (AI), the Internet of Things (IoT), quantum computing, and blockchain present both opportunities and threats. Whilst these technologies can enhance cybersecurity through improved threat detection, automation, and operational efficiency, they also introduce vulnerabilities such as AI-enabled phishing, IoT device exploitation, and risks to traditional cryptographic systems from quantum computing. Furthermore, organizations face significant skills shortages and regulatory challenges, with jurisdictional overlaps and misalignments complicating compliance.

Global disparities in cybersecurity regulations create compliance burdens for multinational organizations, and rapid technological advancements exacerbate this by outpacing regulatory adaptations. Collaborative international frameworks, aligned with technological progress, are necessary to address misalignments and ensure cohesive cyber defense strategies.

To navigate these challenges, the report proposes a structured "MUST" framework: Monitor technological advancements through partnerships and industry engagement; Understand risks and opportunities via impact analyses and pilot testing; Strategize cybersecurity integration aligned with organizational goals and resources; and Transform operations by implementing proven technologies, training employees, and adapting organizational processes.

**As the cyber threat landscape evolves, organizations must adopt adaptive, forward-thinking strategies. By integrating emerging technologies, fostering international collaboration, and addressing workforce challenges, stakeholders can enhance global cybersecurity resilience and ensure robust protection in a rapidly evolving and increasingly interconnected era.**

# 2. Introduction

**As the world experiences a rapid and unprecedented technological revolution, the attack surface has grown dramatically.**

As a result, it has become imperative for cybersecurity to evolve in parallel to protect society from any possibility of disruption caused by cyber threats. To better understand the evolution and future of cybersecurity and address the associated challenges, the Future of Cybersecurity Knowledge Community conducted a comprehensive survey supplemented with expert opinions to ensure a robust and detailed perspective. This combination of quantitative survey data and qualitative expert opinions provides layers of insight and expertise, allowing for the identification of key trends and aiding the forecasting of future developments in cybersecurity.

## 2.1 Overview of the most pressing global cybersecurity challenges

**The evolving cybersecurity landscape requires a multi-pronged approach to meet future challenges, including staying informed about opportunities and threats, collaborative regulatory responses, and continuous upskilling of the cybersecurity workforce.**

For instance, emerging technologies have the potential to enhance cybersecurity measures by improving operations and protecting against sophisticated cyber threats. However, they also introduce new vulnerabilities and attack vectors, complicating the threat landscape. This necessitates regulatory updates and continuous workforce upskilling.

From a regulatory perspective, the primary challenges for international organizations stem from jurisdictional overlaps in cybersecurity regulations. These overlaps arise when multiple policies or regulations related to cybersecurity apply to the same entity but impose differing requirements or directives. This overlapping may occur at various levels, including data protection, privacy, cybersecurity practices and breach notifications.

Additionally, the swift progression of technological innovation is widening cybersecurity workforce challenges, with the demand for new skills outpacing supply. This makes it increasingly difficult for organizations to train and recruit skilled professionals who can effectively navigate the complex ecosystem of modern cyber threats.

Building on the understanding of these pressing challenges, this report addresses three interlinked elements critical to shaping the future of cybersecurity: **technology, international collaboration, and workforce transformation.**

The synergy between these three elements is essential for developing comprehensive and resilient cybersecurity strategies.

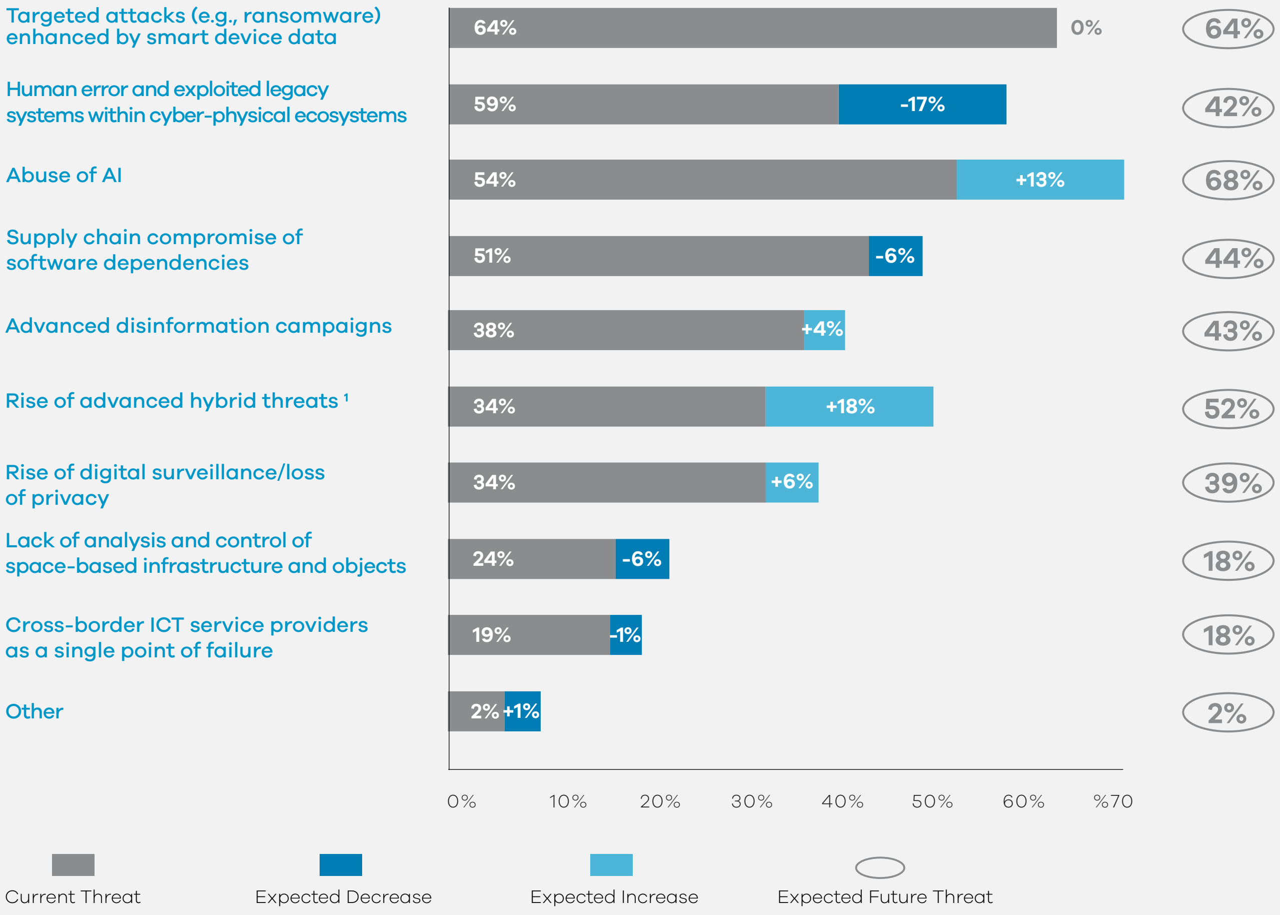
This report analyzes the evolution of cybersecurity through these three lenses, providing valuable insights for professionals and decision-makers in the field, and offering strategies to ensure robust protection in an increasingly interconnected world.

# 3. Technological Acceleration

**Emerging technologies such as AI, IoT, quantum computing and blockchain are not only driving the future of technological advancement but are also significantly impacting the environment in which cybersecurity operates. The evolution of these technologies will reshape the dynamic cybersecurity landscape, resulting in an array of new opportunities and threats.**

## 3.1 Emerging technologies shaping the future of cybersecurity

This assessment is echoed by more than 91% of the experts surveyed in our research, highlighting the impact of a rise in the abuse of AI, advanced threats, digital surveillance and disinformation campaigns as primary determinants of cybersecurity's shifting focus. Meanwhile, the impact of other threats that have historically featured prominently is expected to decline.



Mixture of coercive and subversive activities, conventional and unconventional methods
Note: Numbers might not sum up due to rounding

**Figure 1: Perception of current and future cybersecurity threats for organizations due to emerging technologies**

Additionally, over 95% of respondents recognize cybersecurity's potential as a competitive advantage. Still, 86% believe organizations are not fully prepared to tackle future cybersecurity challenges.

**Survey participants**

95%

**Consider cybersecurity as a competitive advantage**

86%

**Think organizations are not fully prepared for future challenges**

Figure 2: Perceptions of cybersecurity as a competitive advantage and organizational preparedness

This alarming paradox highlights the urgent need for more organizations to become increasingly vigilant and adaptable in their cybersecurity strategies to remain competitive.

Figure 3 shows how organizations that are more aware of more opportunities and threats are increasingly likely to invest in emerging technologies.

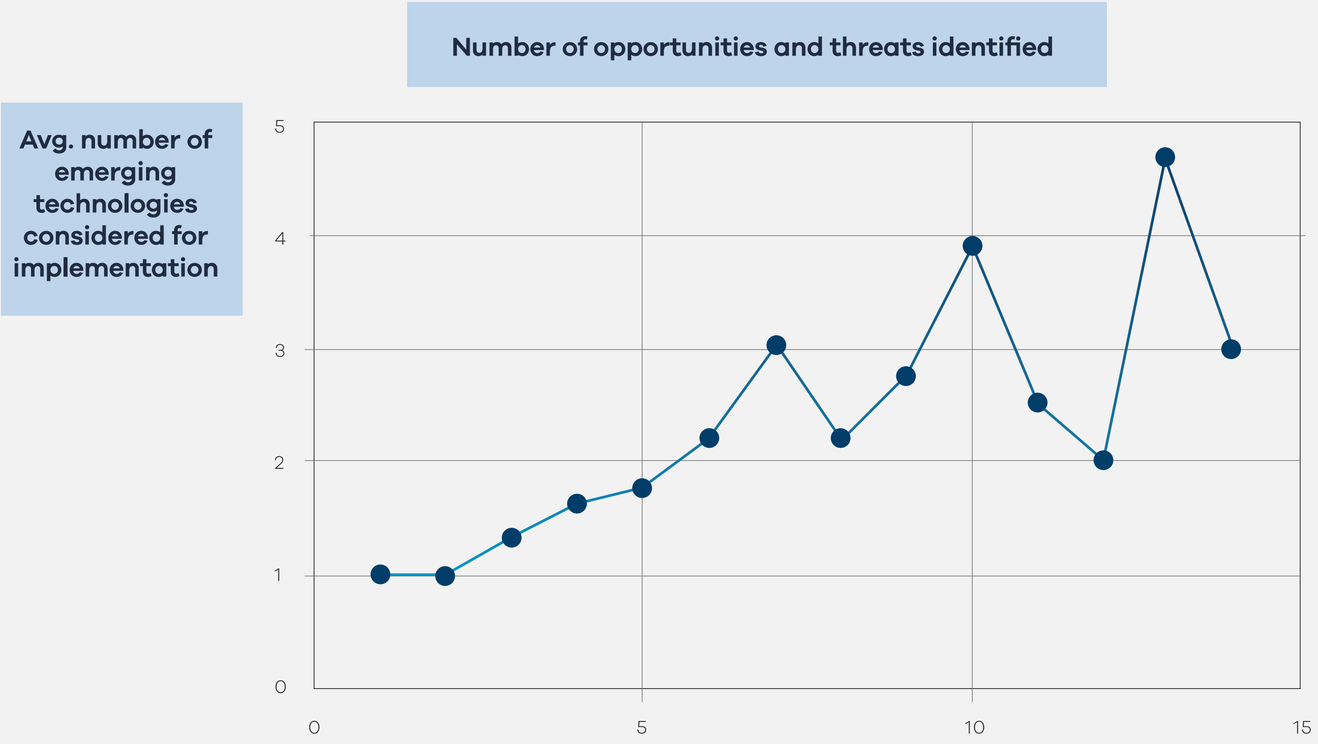


Figure 3: Organizations aware of opportunities and threats tend to invest in emerging technologies

These organizations are responding by investing in emerging technologies, with AI for cybersecurity (89%), IoT security (52%), and secure 5G connectivity (36%) among the most implemented solutions to date. However, while some technologies have demonstrated significant value in their adoption, challenges remain. For instance, quantum computing is still in its early stages of development and has yet to generate meaningful returns on investment. Similarly, blockchain projects often fail to yield significant returns on investment due to unclear value propositions and substantial implementation challenges.

Our survey also revealed that investments in these technologies are limited by skills gaps (69%), the rapid pace of technological innovation (56%), and integration with existing systems (53%). As a result, organizations are prioritizing investments in technologies with proven benefits.

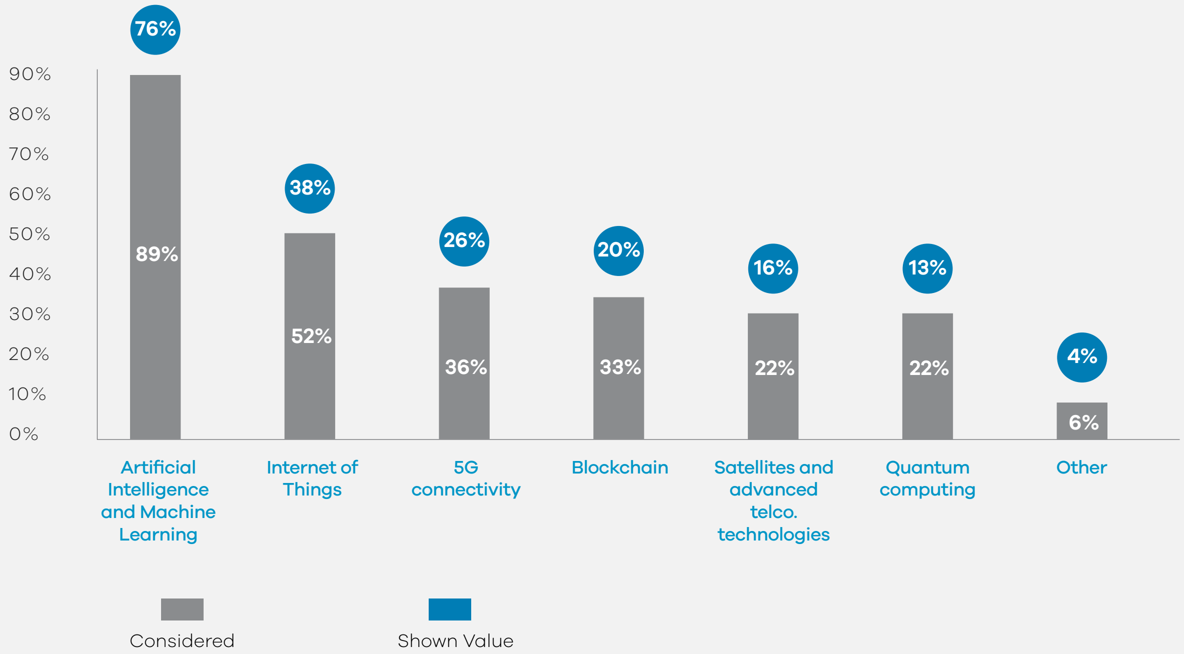


Figure 4: Organizations prioritizing investments in emerging technologies

This chapter aims to enhance understanding of the opportunities and threats emerging technologies present to organizations. By increasing awareness, it seeks to support organizations in making more informed decisions, thereby encouraging improvements in cybersecurity.

### 3.1.1 Transforming cybersecurity with AI

**AI, and generative AI (GenAI) in particular, has garnered significant interest from the wider public for its ability to improve productivity significantly.**

Organizations using GenAI effectively in cybersecurity operations could see up to a 30% increase in operational efficiency[1]. Our research reflects this interest: 89% of the respondents indicated that their organizations are considering AI implementation, and 76% reported that AI has already generated value for their organizations.

The rapid growth of AI has expanded the cybersecurity landscape, introducing both opportunities and threats. On the one hand, AI can enhance cybersecurity by automating threat detection and response. However, it also enables more sophisticated cyberattacks, such as AI-generated phishing emails and malware, that can bypass traditional security measures. This dual nature of AI means that it presents opportunities for cybersecurity defenders and malicious actors[2].

The future of AI in cybersecurity presents numerous opportunities, such as quickly identifying and mitigating threats, reducing response time and improving the overall security posture. Organizations can automate routine security tasks, allowing human experts to focus on more complex issues. Additionally, AI's advanced predictive capabilities enable the prediction of potential threats by analyzing patterns and anomalies in data, allowing for proactive defense strategies. Hence, it is unsurprising that 70% of organizations integrated AI or GenAI into their cybersecurity operations.

However, AI also aids attackers by enabling more convincing phishing campaigns, developing malware that evades traditional security measures, and automating the entire cyberattack lifecycle[3]. The survey indicates that 54% of respondents currently see AI-related cybersecurity risks affecting organizations. This number is expected to grow to 68% in the future. Furthermore, AI systems themselves can be the target of a cyberattack, indicating the need for additional, AI-specific cybersecurity solutions.

Our research highlights varied perceptions around the role AI will play in cybersecurity defense strategies. Enthusiasts believe AI will play a primary role in threat detection and response. The cautious majority see AI as supportive, focusing on specific tasks. Laggards have only just started experimenting with AI. Skeptics believe that the same technology will not play any role in cybersecurity. Despite these differing views, the generally positive perception of AI suggests that reliance on the technology for cyber defense will likely increase soon.

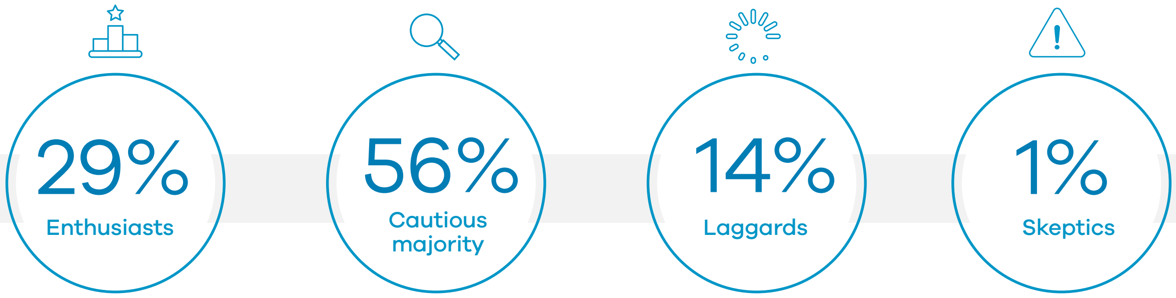


Figure 5: Attitudes toward the role of AI in cybersecurity defense strategies

However, the research also identified concerns related to using AI for cybersecurity, such as misinterpretations and false positives (41%), security vulnerabilities of AI systems (26%), and skill atrophy among staff due to overreliance on AI tools (21%). This means that successful AI implementation would also require changes in ways of working, including:

### Checklist for successful AI implementation

- ✓ Implementing robust monitoring and verification systems to mitigate misinterpretations and false positives
- ✓ Enforcing security procedures to ensure secure integration of AI
- ✓ Introducing continuous training programs to maintain and enhance cybersecurity expertise and capabilities
- ✓ Fostering a working environment that leverages both AI tools and human capabilities to ensure critical thinking and oversight remain essential
- ✓ Establishing feedback mechanisms to allow continuous improvement of AI systems based on real-world performance and user input

### 3.1.2 Unlocking IoT's potential while preserving security

**IoT involves interconnected physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators and connectivity equipment.**

These objects connect and exchange data, enabling more direct integration of the physical world into computer-based systems, leading to improved efficiency, economic benefits, and reduced human exertions.

As shown in Figure 4, the majority of respondents rate IoT as the second most popular emerging technology after AI, indicating it has already shown significant value in their organizations. Unsurprisingly, the future outlook for IoT is highly promising. IoT devices are expected to grow exponentially from 18 billion today to 39.6 billion by 2033[4]. They are driven by increasing business benefits such as providing real-time insights, automating tasks, and creating new revenue streams through innovative services. In industrial environments, IoT can drive major advancements in automation and efficiency. Moreover, advancements in IoT security technologies, such as secure remote access, industrial control system (ICS) network visibility and monitoring, and risk-based vulnerability management, are poised to provide robust frameworks to protect IoT ecosystems.

However, convergence between Information Technology (IT) and Operational Technology (OT) through IoT expands the attack surface of traditionally isolated and secure OT environments, presenting notable cybersecurity challenges. Increased connectivity allows malicious actors to traverse to OT environments via IT networks. As the number of connected devices grows, so does the potential for cyberattacks, especially since many IoT devices lack robust security features, which makes them easy targets. This convergence could lead to attacks on digital systems with severe physical consequences, such as a ransomware attack disrupting a fuel pipeline. Additionally, the proliferation of smart home devices, often with minimal security, poses risks to individual privacy and safety; the delineation of responsibility for IoT security between consumers and businesses further complicates the issue.

To address these threats, businesses must develop and implement a comprehensive risk management approach. Based on the study, such an approach should incorporate IoT-specific security solutions (71%), strict device management policies (66%), regular vulnerability assessments (66%), and network segmentation or air gapping for environment separation (62%).

By incorporating these measures, organizations can more effectively manage the risks associated with IoT while harnessing its potential to drive efficiency and innovation.

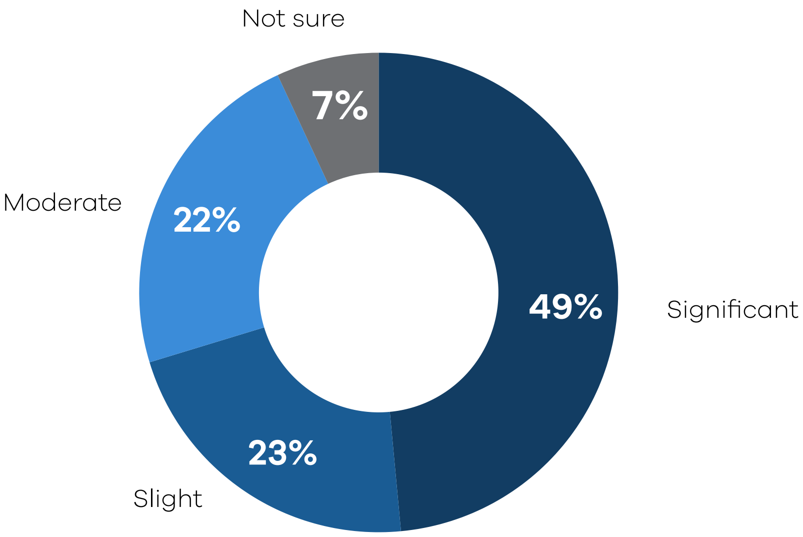
| | |
|---|---|
| IOT-SPECIFIC SECURITY SOLUTIONS | 71% |
| STRICT DEVICE MANAGEMENT POLICIES | 66% |
| REGULAR VULNERABILITY ASSESSMENTS | 66% |
| NETWORK SEGMENTATION OR AIR GAP FOR SEPARATION OF THE ENVIRONMENT | 62% |

Figure 6: Suggested approach for IoT risk management

### 3.1.3 Quantum computing: A business opportunity and cybersecurity challenge

**Quantum computing represents a major shift from classical computing, leveraging quantum mechanics to process information in dramatically different ways.**

Although the development of a general-purpose quantum computer remains uncertain, with estimates suggesting it could take over 20 years, most respondents (49%) believe that quantum computing will significantly impact encryption within the next five years. This is mirrored in the fact that research and progress in the technology continues to grow – between 2020 and 2023, the number of patents related to its development approximately doubled from 1,899 to 3,795.[5]



Note: Numbers might not sum up to 100 due to rounding

Figure 7: Expected impact of quantum computing on encryption over the next five years

#### Opportunities in cybersecurity

Quantum technology presents significant opportunities for the future of cybersecurity:

**Optimization:** Quantum computing can solve some complex problems more efficiently than classical computers, leading to cost savings and enhanced decision-making. This capability can reduce risks and vulnerabilities in cyber operations.

**Simulation:** Quantum simulations can more accurately model cyber threats and defenses, aiding in developing robust security measures.

**Parallelization:** The ability to perform multiple computations simultaneously is crucial for threat detection and monitoring large-scale networks.

**Advanced encryption:** Quantum computing also offers new avenues for enhancing security through advanced encryption techniques, providing stronger protection for sensitive data.

#### Challenges to cybersecurity

**However, this emerging technology also poses significant cybersecurity threats:**

**Breaking cryptographic systems:** Quantum computing has the potential to disrupt existing cryptographic systems, such as Rivest–Shamir–Adleman (RSA) and elliptic curve cryptography, which are the cornerstones of modern cryptography.

**'Harvest now, decrypt later' attack:** Attackers may collect encrypted data today to decrypt in the future when quantum computers are more advanced. This threat jeopardizes the digital economy, which relies on cryptography to secure information exchange.

**Compromised sensitive data:** Sensitive data, including financial and personal information, could be compromised, leading to financial losses and a general loss of trust.

Implementing quantum-safe cryptography is essential to maintain the integrity of digital trust mechanisms and ensure ongoing cybersecurity. However, our research shows that monitoring current developments and planning accordingly (68%), as well as engaging with cybersecurity consortia for quantum readiness (63%), are preferred approaches over investing in quantum-resistant cryptography (47%). In addition to these measures, transitioning to quantum-safe cryptography remains critical. As dependency on cryptographic security grows, ensuring the robustness of digital trust mechanisms through adopting quantum-safe cryptographic methods is essential to maintaining the overall security of Cyberspace.

### 3.1.4 Blockchain technology as a tool to mitigate cyber fraud

**Blockchain is revolutionizing the exchange of value, much like the internet did for the exchange of information. As a decentralized ledger technology, blockchain records transactions across multiple computers, ensuring that registered transactions cannot be altered retroactively.**

This transparency and security make blockchain resistant to data tampering and fraud, with transactions validated by network participants rather than a central authority. In cybersecurity, blockchain is a powerful tool for mitigating and prosecuting cyber fraud. The traceability of blockchain transactions provides a significant advantage. For instance, law enforcement agencies can trace and apprehend cybercriminals by following digital trails left by cryptocurrency transactions. Moreover, blockchain's transparency and immutability secure data integrity, prevent unauthorized access, and ensure the safety of digital assets.

Beyond securing transactions and payment systems, blockchain significantly benefits identity verification and access management. It also enhances supply chain security and origin tracking, ensuring that products are authentic and have not been compromised during the supply chain process.

If implemented properly, blockchain has immense potential for future cybersecurity applications. Emerging Web3 technologies can unlock new use cases across various sectors, increasing transparency and fostering direct relationships between businesses and customers. Blockchain can decentralize the business world by enabling community ownership. Additionally, transferring funds instantly across borders without bureaucratic hurdles offers considerable advantages, making the global economy bigger, fairer, and more integrated.

However, blockchain technology is not immune to cybersecurity threats despite its robust security features. As a nascent technology, it is open to undiscovered vulnerabilities, presenting risks that may still need to be identified or fully understood. Key threats include:

**51% attacks:** Where a group of 'miners' controls more than 50% of the network's computing power, enabling them to manipulate the blockchain.

**Phishing attacks and theft:** Attackers gaining unauthorized access to private keys or digital wallets where digital assets and cryptocurrencies are stored.

**Smart contract vulnerabilities:** Bugs or flaws in the smart contract code can be exploited by malicious actors.

Prioritizing cybersecurity is essential to mitigate these risks and ensure the safe deployment of blockchain applications across various sectors. For instance, implementing cybersecurity solutions that provide real-time monitoring of blockchain transactions can help identify suspicious activities and uncover illicit networks.

## 3.2 Cybersecurity threat landscape and best practices in 2025

Building upon the previous discussion of how emerging technologies are reshaping Cyberspace, this section prioritizes associated threats and risks according to severity and likelihood of occurrence.

**Top technologies impacting the threat landscape in 2025**
In the survey, respondents identified the emerging cybersecurity threats they are most concerned about for 2025. In Figure 8, these technologies are ranked according to the severity of the cybersecurity threats they are expected to pose. The top three technologies expected to impact Cyberspace in 2025 are:

**1) AI-powered cyberattacks:** The advancement of AI technology enables more sophisticated and automated cyberattacks. These AI-driven attacks can adapt and learn from defenses, making them particularly challenging to counteract.

**2) IoT vulnerabilities:** The proliferation of IoT devices introduces numerous security vulnerabilities. Many IoT devices lack robust security measures, making them easy targets for attackers to exploit.

**3) 5G network threats:** The widespread adoption of 5G networks introduces new security risks. The increased connectivity and speed of 5G make networks more vulnerable to cyberattacks and espionage activities.

| Rank | Technology |
|---|---|
| 1 | AI-POWERED CYBER ATTACKS |
| 2 | IOT VULNERABILITIES |
| 3 | 5G NETWORK THREATS |
| 4 | SATELLITES AND OTHER ADVANCED TELCO. THREATS |
| 5 | QUANTUM COMPUTING THREATS TO CRYPTOGRAPHY |
| 6 | BLOCKCHAIN-RELATED THREATS |

Figure 8: Cybersecurity technologies ranked according to the severity of the threats they are expected to pose in 2025

**Best practices for 2025**

To address these and other evolving threats, the study has identified three best practices that can improve cybersecurity in 2025:

**1) Zero Trust Network Access (ZTNA):** This security model assumes no trust by default, regardless of whether the user is inside or outside the network perimeter. It enforces strict identity verification for every individual and device attempting to access resources.

**2) Secure-by-design principles:** Integrating security into the design and development process from the outset ensures that systems and applications are built with security considerations in mind. This proactive approach reduces vulnerabilities and enhances the overall security posture.

**3) Continuous authentication:** Continuously verifying user identity throughout a session rather than just at login can help detect and prevent unauthorized access by monitoring user behavior and detecting anomalies in real time.

| Rank | Best Practices |
|---|---|
| 1 | ZERO TRUST NETWORK ACCESS (ZTNA) |
| 2 | CONTINUOUS AUTHENTICATION |
| 3 | SECURE-BY-DESIGN PRINCIPLES |
| 4 | PRIVACY-ENHANCING COMPUTATION |
| 5 | DECENTRALIZED IDENTITY MANAGEMENT |

Figure 9: Cybersecurity best practices for 2025

The alignment of best practices with identified threats indicates that cybersecurity specialists have a strong understanding of how to combat the increasing sophistication of cyber threats effectively. However, organizations must be proactive and adopt comprehensive security measures to avoid potential attacks and protect critical assets.

## 3.3 Recommendations to strengthen future cybersecurity postures

In a rapidly evolving digital landscape, integrating emerging technologies into cybersecurity strategies is not an option but a necessity. This report proposes a structured approach (MUST – Monitor, Understand, Strategize, and Transform) for organizations to stay on top of emerging cybersecurity trends, and thus supports them in enhancing their future cyber postures.

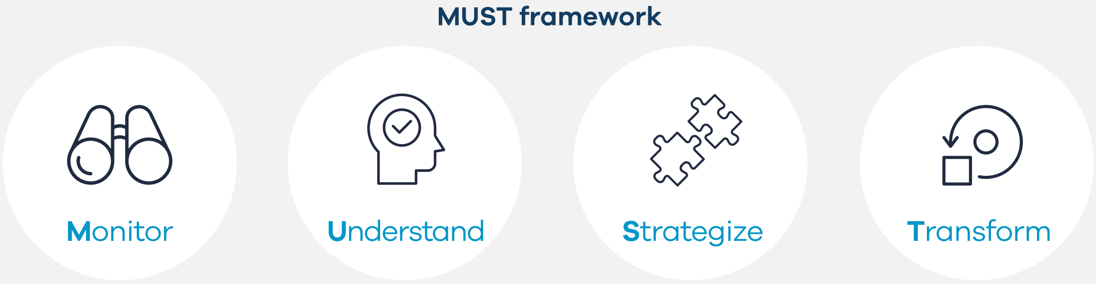


Figure 10: MUST framework

**Monitor:** Continuously track the evolution of emerging technologies to stay on top of current and future trends in cybersecurity

**Internal foresight:** Establish robust systems and assign team responsibility for monitoring the development and adoption of emerging technologies (e.g., AI, IoT, quantum computing, etc.) by scanning leading industry publications (e.g., Gartner Hype Cycle).

**Partnerships and alliances:** Establish strategic partnerships with vendors, research institutions, and peers to stay ahead of technological advancements. Leverage these partnerships to gain access to cutting-edge cybersecurity solutions and insights.

**Engage with industry:** Actively participate in leading industry events (e.g., forums, webinars, and conferences) to stay updated on the latest trends, innovations, and best practices in cybersecurity.

**Understand:** Develop a deep understanding of how emerging technologies impact the cybersecurity landscape and what they can bring to your organization

**Impact analysis:** Continuously reevaluate potential risks and benefits that emerging technologies may bring to your organization in terms of cybersecurity and broader business context to identify promising applications. These assessments should focus on the present and future for appropriate strategic planning. For future state assessments, developing science-based foresight scenarios is crucial.

**Pilot testing:** Validate potential benefits and challenges promising technologies and applications might bring to your organization through tests in a controlled environment. Collect data and insights from these tests to inform decision-making and refine the approach before wider implementation.

**Strategize:** Embrace emerging technologies for cybersecurity through:

**Strategic planning:** Base findings from the Monitor and Understand phases to formulate a strategic roadmap that incorporates the adoption and integration of emerging technologies into the existing cybersecurity infrastructure. Align this roadmap with the organization's overall business strategy.

**Financial planning:** Allocate resources and budget for the research, testing and implementation of emerging technologies. Ensure investments align with the organization's risk appetite and strategic priorities.

**Transform:** Implement and adapt emerging technologies to transform and strengthen the organization's cybersecurity posture

**Technology integration:** Implement and scale technologies that have proven the potential to fortify cybersecurity posture and bring value to your organization.

**Workforce:**

- Invest in training cybersecurity employees to ensure they are equipped with necessary skills and prepared for new ways of cyber defense
- Improve awareness among all employees regarding cybersecurity opportunities and threats emerging technologies can bring today and in the future

**Processes and organization:** Align processes and organizational structures to support integrating emerging technologies.

Integrating emerging technologies into cybersecurity strategies is essential for maintaining a robust security posture in a dynamic digital environment. Organizations can proactively manage cybersecurity risks by adopting the MUST framework and leveraging new technologies to enhance their defenses. This structured approach ensures that organizations are better prepared for current threats and well-positioned to capitalize on future technological advancements for improved security outcomes.

# 4. International Collaboration: Regulatory Frameworks

**Cybersecurity transcends technological boundaries and is deeply intertwined with regulatory frameworks. As cyber threats evolve in complexity and scale, international organizations face the daunting challenge of protecting digital infrastructures while navigating a mosaic of international regulations.**

This chapter analyzes the current challenges that lie at the intersection of cybersecurity and current regulatory frameworks. It explores the multifaceted nature of cybersecurity across different jurisdictions, delving into the global diversity of cybersecurity regulations and standards. By highlighting how disparate regulatory landscapes contribute to complex cybersecurity challenges, the report underscores the significant overlaps and risks posed by the need to maintain a secure global digital environment, further emphasizing the necessity for coherent and unified regulatory frameworks. The ongoing tension between regulatory frameworks and rapid technological advancements is also addressed with a closer look at the role of collaboration and international cooperation. The chapter concludes with an overview of threats, trends, and opportunities for policy makers and industry leaders.

This in-depth analysis is designed to equip policymakers, industry leaders, and security experts with insights and strategies for navigating the evolving cybersecurity landscape. It aims to ensure robust defense mechanisms that align with international regulations and promote global digital stability.

## 4.1 Current challenges in the context of regulatory frameworks

Global cybersecurity laws and regulations pose significant compliance challenges for multinational companies because they vary in definitions, scopes, and application areas, complicating the development of a unified compliance strategy. Rapid technological advancements further exacerbate these challenges, as regulatory frameworks often need help keeping pace with the development of emerging technologies.

### 4.1.1 Global diversity in cybersecurity regulations

Some cybersecurity laws and regulations encompass all aspects of information security, while others focus narrowly on specific areas like data protection or critical infrastructure.

There are also vast issues in how some regulations are tailored to specific industries or sectors, such as finance and healthcare, while others are more generic.

Regional variations further complicate compliance efforts. Data privacy regulations best illustrate this. In Europe, for instance, the General Data Protection Regulation (GDPR)[6] sets strict requirements for protecting personal data, with significant penalties for non-compliance. In the United States (US), laws like the Health Insurance Portability and Accountability Act (HIPAA)[7] and the Gramm-Leach-Bliley Act (GLBA)[8] are responsible for regulating data protection in specific sectors. At the same time, broader regulations like the California Consumer Privacy Act (CCPA)[9] and other state breach notification laws also apply. In Asia, countries like China have enacted cybersecurity laws with stringent data localization requirements, while others, such as Japan, have adopted guidelines based on international standards.

Varying definitions and scopes of cybersecurity laws make it challenging for multinational corporations to develop a unified compliance strategy, leading to increased costs and administrative burdens. Therefore, these companies must adopt flexible, adaptive cybersecurity strategies to ensure compliance and mitigate regulatory risks.

### 4.1.2 Jurisdictional overlaps and misalignments

**Jurisdictional overlaps arise when different cybersecurity regulations apply to the same entity or incident but provide differing requirements or directives.**

These misalignments can occur on sectoral, national, and international levels and involve various issues, from data protection and privacy, to cybersecurity practices and breach notifications.

This can lead to practical problems such as hindering the mechanism of effective international cooperation in fighting cybercrime, violating the fundamental principle of ne bis in idem (by which a person cannot be punished and be subject to several procedures twice for the same facts) and duplicating efforts by policy enforcement officials of the involved entities.

Different sectors often have unique cybersecurity measures, complicating compliance for businesses active across multiple industries or regions. For instance, the financial industry typically faces more rigorous data protection and incident reporting rules than the retail sector.

Moreover, enforcing cybersecurity regulations across various jurisdictions can spark legal disputes about which entities' regulations take precedence. Companies operating internationally frequently struggle to navigate these misaligned regulatory requirements, leading to uncertainties in legality, challenges in compliance, and shortcomings in effectively mitigating cyber threats. Addressing these issues necessitates national and international cooperation, harmonization of cyber policies and regulations when applicable, and the creation of unified frameworks and standards. Organizations operating internationally should keep abreast of regulatory adjustments and adopt an integrated, transnational strategy for cybersecurity compliance.

### 4.1.3 Regulatory frameworks versus technological advancements

**Rapid technological advancements pose significant challenges for existing legal systems, particularly those concerning cybersecurity and privacy.**

The widening gap between technological progress and legal adaptation creates concerns about privacy, security, and the ethical use of technology. The gap highlights the need for regulatory frameworks that are both flexible and responsive to new realities. It is important to continue developing cybersecurity policies, with our research finding that 70% of the respondents view policies and regulations as effective tools in addressing cybersecurity challenges.

70%

**of the respondents view policies and regulations as effective tools in addressing cybersecurity challenges**

A comparative analysis of regulatory responses to technological advancements reveals interesting insights into how different jurisdictions address the challenges posed by AI, IoT, and other emerging technologies.

In the European Union (EU), regulations like the GDPR have been implemented to safeguard individuals' privacy and data rights in the digital age. Additionally, the EU has proposed the Artificial Intelligence Act, which aims to establish a comprehensive framework for AI regulation, focusing on transparency, accountability, and ethical use.

In Saudi Arabia, the Saudi Data and AI Authority (SDAIA) has issued AI Ethics Principles and Generative Artificial Intelligence Guidelines for government use. The AI Ethics Principles are a practical guide for integrating ethical considerations throughout the AI system development life cycle. Meanwhile, the Generative AI Guidelines provide regulatory instructions for government employees on using and processing government data in generative AI tools.

In the US, regulatory responses have been more varied, with various agencies addressing specific aspects of technology regulation. For instance, the Federal Trade Commission (FTC) enforces consumer protection laws concerning data privacy and security. At the same time, the National Institute of Standards and Technology (NIST) provides guidelines for cybersecurity and AI ethics.

While each jurisdiction has tried to adapt its regulatory frameworks to technological advancements, significant variance in approaches and priorities still needs to be addressed. Collaborative efforts, knowledge sharing, and international standards development could help bridge the gap and promote more consistent and effective regulation across borders.

## 4.2 Top regulatory trends in 2025

**As outlined in the previous section, the rapid advancement of technologies and the diversity of regulatory approaches have created a complex landscape for cybersecurity. This evolving landscape is characterized by several key threats and trends shaping its future.**

Among the primary trends influencing the future of cybersecurity regulations are digital sovereignty, proactive cybersecurity regulation, continuous risk management regulation, and regulating increasingly connected sectors.

As a result of geopolitical circumstances, nations striving for digital sovereignty increasingly focus on enhancing cyber capabilities and fostering selected partnerships. Additionally, there is a notable shift towards adaptable, principle-based frameworks that balance innovation with security. These frameworks emphasize continuous risk management tailored to specific organizational contexts. The proliferation of IoT and connected devices has expanded the cyberattack surface, requiring comprehensive, sector-specific regulatory measures.

### Rise of digital sovereignty

Efforts to achieve digital sovereignty are intensifying, with regulations and policies evolving to support these initiatives. In the coming years, regulations are expected to focus on enabling nations to develop sovereign cyber capabilities, strengthening digital public infrastructure, and implementing export restrictions to maintain competitive advantages and protect sensitive information. Monitoring cross-border data flows will also be crucial to defending against external threats and influences.

Collaboration between technological advancement and regulatory frameworks will likely be strengthened to achieve digital sovereignty. This will involve integrating cybersecurity into global trade agreements and enhancing the cyber maturity of global allies through collaborative efforts and information sharing. Countries can maximize joint research and innovation by forging selective strategic partnerships, bolstering their collective cybersecurity capabilities.

### Proactive cybersecurity regulation

An increasing emphasis on balancing security and innovation in proactive cybersecurity regulations is another significant trend.  Given the rapid evolution of emerging technologies, such as quantum computing, regulators are adopting a proactive stance to defend against future vulnerabilities in Cyberspace and shape the future of cybersecurity. This trend is expected to grow. Investing in predictive technologies and adaptable frameworks ensures cybersecurity policies remain forward-thinking and robust. There is a strong emphasis on securing emerging technologies through stringent standards and secure-by-design principles. This forward-looking approach, aimed at effectively managing economic viability and cybersecurity risks, is anticipated to drive the evolution of cybersecurity regulation in the coming years.

### Continuous risk management regulation

Due to the fast-paced technological advancement and evolving threat landscape, continuous risk management will likely become a new regulatory approach. There is a notable shift from point-in-time compliance-based regulation towards continuous risk management-focused regulation as organizational maturity increases across nations. Traditionally, regulators would prescribe a set of requirements that companies needed to implement, often not tailored to organizational context and risk profiles. This promoted a culture of compliance-focused maturity, as organizations aimed to demonstrate compliance during annual audits but did not maintain measures to mitigate risks.

However, as companies mature, regulators are now emphasizing the creation of risk management frameworks tailored to specific organizational contexts and risks. This approach ensures that companies continuously monitor and address potential risks, addressing their major vulnerabilities. Regulators are increasingly expecting companies to manage risks continuously, ensuring consistent and comprehensive risk mitigation rather than just focusing on periodic inspections. As cybersecurity maturity increases across organizations, this approach is expected to become more prevalent in the future.

### Regulating increasingly connected sectors

The proliferation of IoT and connected devices across various industries has expanded the cyberattack surface, creating new vulnerabilities and evolving threat landscape. Sectors previously less exposed to cyber threats, such as agriculture, automotive, aviation, and energy, now face complex challenges due to increasing connectivity opening vulnerabilities that cybercriminals can exploit, increasing the risk of cyberattacks.

There is a growing and urgent need for robust cybersecurity regulations to enhance the cybersecurity posture of these sectors. This entails not only the implementation of stringent security measures but also the continuous monitoring and updating of these measures to adapt to the evolving threat landscape. A collaborative and coordinated approach is essential to address these emerging risks and safeguard critical sectors effectively.

Cybersecurity regulators must work with sector-specific regulators, industry stakeholders and other relevant entities to develop comprehensive and effective solutions. These solutions should be tailored to each sector's unique needs and vulnerabilities, ensuring that all potential threats are adequately mitigated. By joining forces and pooling their expertise and resources, regulators can create robust cybersecurity frameworks that protect these vital sectors from ever-increasing cyber threats.

## 4.3 The role of collaboration in cybersecurity regulations

**Findings from our research indicate that collaboration is a crucial factor in advancing cybersecurity initiatives, with 94% of respondents highlighting its importance. This is especially true for collaboration on cybersecurity regulations, particularly in aligning regulatory frameworks.**

Inadequate security in one country can have far-reaching consequences for others, underscoring the need for international collaboration in cybersecurity regulations. Such collaboration provides multinational companies with a more coherent regulatory framework, facilitating navigation through the complexities of cybersecurity regulations. Additionally, collaboration can significantly enhance the overall cybersecurity posture of organizations by enabling the sharing of cybersecurity capabilities

94%

**Perceive collaboration as an important factor for advancing cybersecurity**

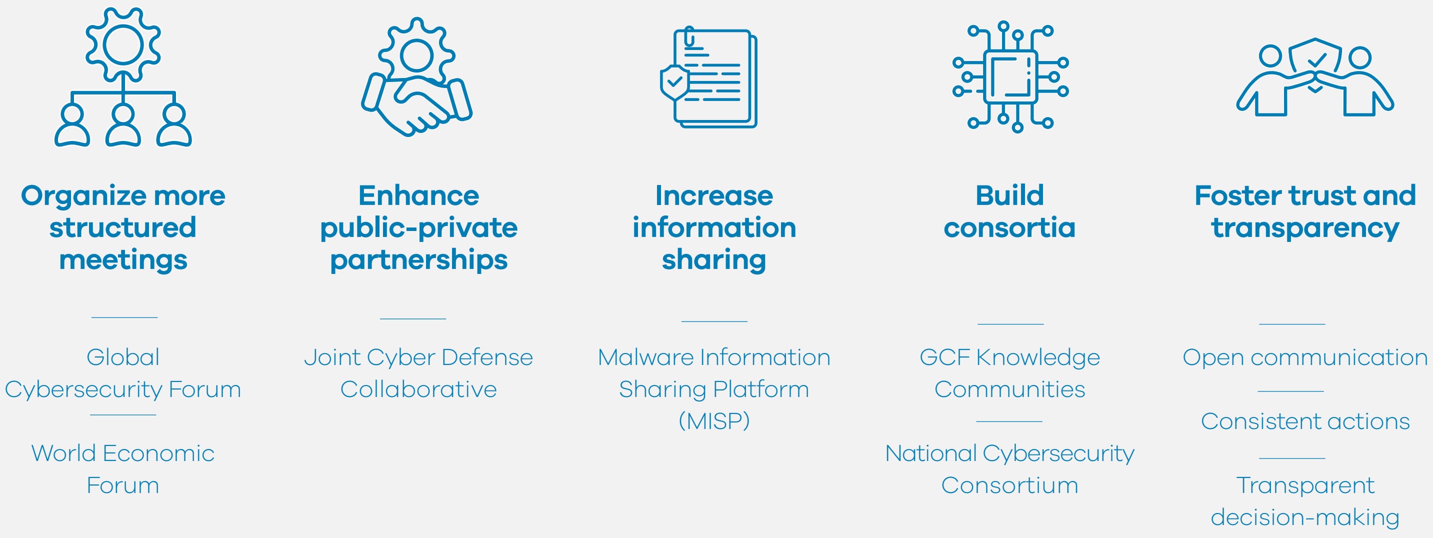
Engaging in discussions and articulating common legal principles is important to promote and regulate cybersecurity effectively. While cybersecurity regulations may vary, international coordination can enhance their efficacy by providing consistency and enabling policymakers to learn from successes and failures in other countries. The interconnected nature of cyber threats further emphasizes the importance of global cybersecurity regulations. Collaborative and cooperative frameworks can prove vital by incorporating incentives, public-private partnerships and tailored regulations to improve cybersecurity holistically.

Achieving a global cybersecurity regulatory framework involves modernizing cybersecurity laws and regulations, ensuring uniformity of legal requirements, coordinating cooperative programs, and focusing on supply chain security. Nations can promote cybersecurity measures by enacting effective regulations and fostering public-private partnerships. While complete global uniformity is impractical due to differing legal constraints and values, some cohesion can provide companies with more effective pathways to comply with the patchwork of global laws and regulations. International dialogue and best practices can facilitate the sharing of critical threat information and improve cyber threat information-sharing programs globally.

Examples of initiatives that enhance cybersecurity collaboration include the Global Cybersecurity Forum (GCF)[10] and the Center for Cybersecurity of the World Economic Forum (WEF)[11]. These initiatives serve as platforms where policymakers and experts meet, exchange knowledge, learn from each other's experiences, and strengthen the collective response to cyber threats. In addition to facilitating discussion, they conduct research and publish reports to spread the message and awareness about the latest advancements in cybersecurity. By sharing best practices and promoting collaboration, these initiatives contribute to formulating effective cybersecurity regulations and standards globally.

Collaboration in cybersecurity delivers benefits to organizations beyond uniform policies and regulations. These benefits include enhanced threat intelligence, accelerated incident response, and cost savings. Organizations can leverage collaboration to exchange threat intelligence, encompassing indicators of compromise, attack methodologies, and emerging trends. By merging their collective knowledge, organizations can attain a holistic comprehension of the threat landscape. Consequently, this can facilitate proactive defense measures against novel and advanced attacks.

Collaboration also expedites incident response and recovery in a cyber incident. Setting up reliable and secure channels for collaboration allows organizations to exchange up-to-the-minute data regarding active attacks and collaborate to mitigate their effects. This instant collaboration results in quicker response times, curtailing damage and operational downtime. Additionally, collaboration in cybersecurity can lead to cost savings for organizations. This diminishes the probability of threat actors successfully penetrating company networks, safeguarding against expensive breaches and attacks.


**Organize more structured meetings**

Global Cybersecurity Forum

World Economic Forum

**Enhance public-private partnerships**

Joint Cyber Defense Collaborative

**Increase information sharing**

Malware Information Sharing Platform (MISP)

**Build consortia**

GCF Knowledge Communities

National Cybersecurity Consortium

**Foster trust and transparency**

Open communication

Consistent actions

Transparent decision-making

Figure 11: Actions to enhance collaboration

## 4.4 Recommendations for policymakers and industry leaders

### 4.4.1 Recommendations for policymakers

**The exponential growth and development of disruptive innovation poses significant challenges for policy makers across various industrial fields.**

These challenges revolve around keeping pace with technological advancements (from a regulatory perspective) and reducing the gap between emerging new technologies and developing and enforcing regulations. Designing a regulatory framework that prioritizes public security and privacy while fostering a feasible commercial use and customer satisfaction is increasingly challenging, given the acceleration of technological evolution. To address this, approaches, tools, and methodologies should be adopted to respond to rapid technological advancements and reduce the regulatory gap.

Anticipatory regulations

Regulatory sandboxes

Regulatory impact assessment

International collaboration

Education and training

Figure 12: Recommendations for policy makers

### Anticipatory regulations

The conventional methods of issuing regulations need help to keep up with the speed of technological advancements. Anticipatory regulation is a dynamic approach that is proactive, iterative, and adjusts to the changing landscape of industries and markets. This approach aims to provide attributes and tools that support regulators in identifying, building, and testing solutions to address emerging regulatory challenges. This includes monitoring emerging technology, conducting technology assessments, scenario-planning, and horizon-scanning to address potential risks, challenges, and ethical concerns proactively. The MUST framework may be well-suited to support these efforts.

### Regulatory sandboxes

Regulatory sandboxes are tools that allow businesses to experiment and test new and innovative products, services, or business models under the direct supervision of a regulator. These sandboxes foster business learning by developing and testing technologies and innovations in a real-world environment. They also support regulatory learning by formulating experimental legal systems that guide businesses throughout their innovation activities under the supervision of the regulatory authority.

### Regulatory impact assessment

Conducting frequent regulatory impact assessments helps evaluate the effectiveness of controls and regulations and determines the need for new regulatory measures in response to technological developments. This systematic approach assesses the positives and negatives of proposed and existing regulatory and non-regulatory alternatives. It also supports policymakers in making informed decisions, ensuring the effectiveness of regulations, and minimizing adverse effects on affected parties.

### International collaboration

Given the rapid pace of technological advancement, there is an increasing need for international regulatory collaboration. Collaborative efforts among countries can help develop and harmonize regulations to tackle global challenges posed by emerging technology. This involves sharing information, aligning regulatory approaches, and promoting and adopting consistency across borders to foster innovation while ensuring safety, security, and ethical considerations. International collaboration includes exchanging best practices, conducting joint research initiatives, and establishing mutual recognition agreements. Such efforts enhance regulatory efficiency, minimize duplications of efforts, and tackle transitional issues arising from rapid technological growth more effectively.

### Education and training

Regulators should invest in education and training for their affiliates to facilitate a solid understanding of emerging technologies, such as AI, blockchain, biotechnology, and IoT. Regulatory educational programs should also provide a robust foundation in regulatory theory, policy analysis, risk assessment, and enforcement strategies, including understanding regulatory frameworks, legal principles, and the overall regulatory lifecycle. By investing in a comprehensive and robust training and education program, regulators can improve their capacity to understand, evaluate, and respond effectively to rapid technological advancements.

## 4.4.2 Recommendations for industry leaders

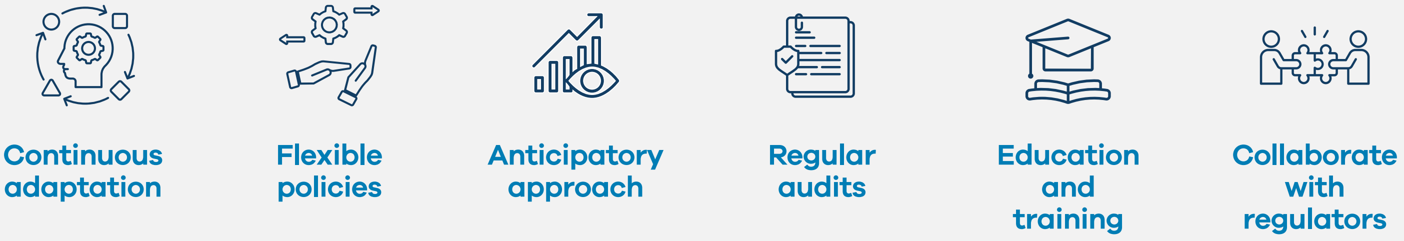


Figure 13: Recommendations for industry leaders

### Continuous adaptation

Most of the participants in this research (79%) believe that the best approach for organizations to respond to an ever-evolving environment is to diligently monitor ongoing legislative developments and emerging risks. By staying ahead of these changes, companies can proactively update their policies to ensure compliance with new regulatory frameworks. This continuous vigilance can mitigate potential legal pitfalls and positions organizations to adapt swiftly to regulatory shifts, fostering a culture of compliance and resilience and enabling organizations to navigate complex regulatory frameworks with confidence and agility.

79%

**Consider diligently monitoring ongoing legislative developments and emerging risks as the best approach to respond to evolving regulations**

### Flexible policies

Organizations should draft flexible policies focused on principles that apply across technologies and jurisdictions, ensuring they are adaptable to various environments. As new innovations emerge, these policies can be easily updated by emphasizing fundamental principles rather than specific technologies and jurisdictions. This approach benefits organizations by facilitating swift compliance with evolving regulations, reducing non-compliance risk. It also ensures that policies remain relevant and effective, enabling organizations to maintain robust security and privacy standards in a dynamic regulatory landscape.

### Anticipatory approach

Organizations should anticipate relevant technical advancements and incorporate them into policy design to create effective, forward-looking policies as new technologies arise. This approach ensures that organizations stay ahead of regulatory changes, reducing non-compliance risk and enhancing their ability to adapt quickly to technological shifts.

### Regular audits

Conducting regular audits helps identify areas where regulatory conflicts may arise and provides insights for proactive adjustments. This proactive approach enables organizations to perform timely corrections, mitigating non-compliance risks. Regular audits also demonstrate a commitment to regulatory adherence, enhancing organizational reputation and trust.

### Education and training

Implementing comprehensive education and training programs focused on cybersecurity, data privacy, and regulatory compliance benefits organizations by enhancing employees' awareness and understanding of compliance requirements, thereby reducing the risk of non-compliance. It also fosters a culture of vigilance and accountability, ensuring that all staff are equipped to handle regulatory challenges effectively.

### Collaborate with regulators

Organizations can proactively engage with regulators by participating in consultations, providing feedback on proposed regulations, and joining industry advisory groups. This collaboration ensures organizations are well-informed about upcoming regulatory changes, allowing for timely adjustments to compliance strategies. By fostering strong relationships with regulators, organizations can influence the development of practical and effective regulations, ultimately reducing compliance risks and enhancing their reputation for regulatory adherence.

# 5. Workforce Transformation

**In the rapidly evolving cybersecurity landscape, the importance of the human element cannot be overstated. While technological solutions are essential for protecting against cyber threats, the effectiveness of cybersecurity ultimately depends on the people who design, implement, maintain and operate those solutions.**

As technology evolves, so must the workforce to ensure effective protection. In our study, 95% of respondents said they believe a cybersecurity workforce transformation has already started, primarily driven by technological evolution and technological advancements, followed by organizational needs and compliance with national cyber strategies. This indicates that workforce transformation is not uniform but heavily dependent on the context in which an organization operates, such as industry, country and cybersecurity maturity.

95%

**of 180 respondents believe the cybersecurity workforce transformation has begun**

| | |
|---|---|
| EVOLVING CYBER THREATS | 76% |
| TECHNOLOGICAL ADVANCEMENTS | 71% |
| ORGANIZATIONAL NEEDS AND PRIORITIES | 54% |
| COMPLIANCE WITH NATIONAL CYBER STRATEGIES | 51% |

Figure 14: Factors perceived to be driving workforce transformation

## 5.1 Understanding the why and how of cybersecurity workforce challenges

**The workforce shortage and skills gap are metrics often used to assess the state of the cybersecurity workforce. 'Workforce shortage' refers to the disparity between the demand for cybersecurity professionals and their availability.**

Recent findings show that globally, the cybersecurity workforce shortage stands at 2.8 million professionals or approximately 39% of the current cybersecurity workforce.[1] However, having more cybersecurity professionals is not enough; their skills are equally important. A skills gap metric measures a mismatch between skills needed by organizations and available (both within and outside of the organization).

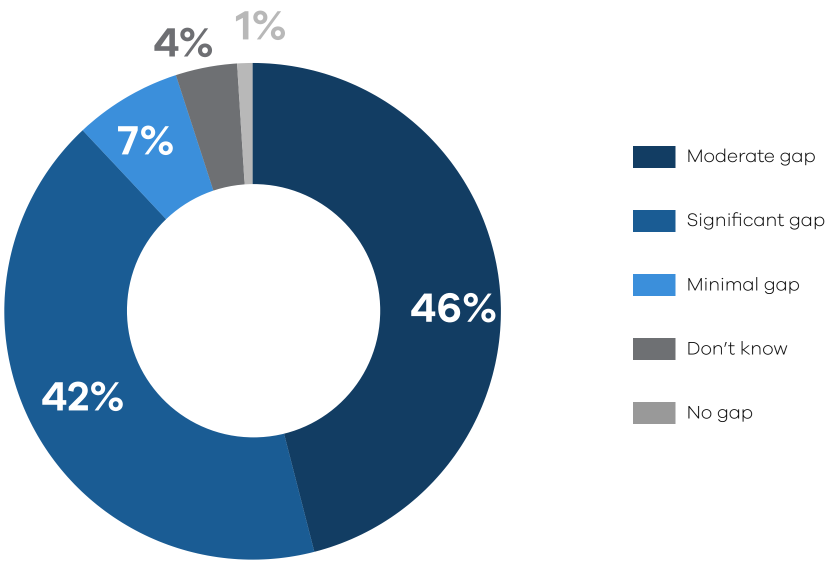


Figure 15: The current skills gap in the cybersecurity domain

Our research highlights the magnitude and importance of the skills gap issue. More than 95% of the respondents believe organizations face a skills gap, and over 42% believe a significant one exists. As illustrated in Figures 16 and 17, the exact gap in expertise and skills depends heavily on the organization's cybersecurity maturity and the context in which it operates, making it difficult to provide a one-size-fits-all solution. However, in the following sections, we have identified best practices that organizations can implement to better prepare for the future.

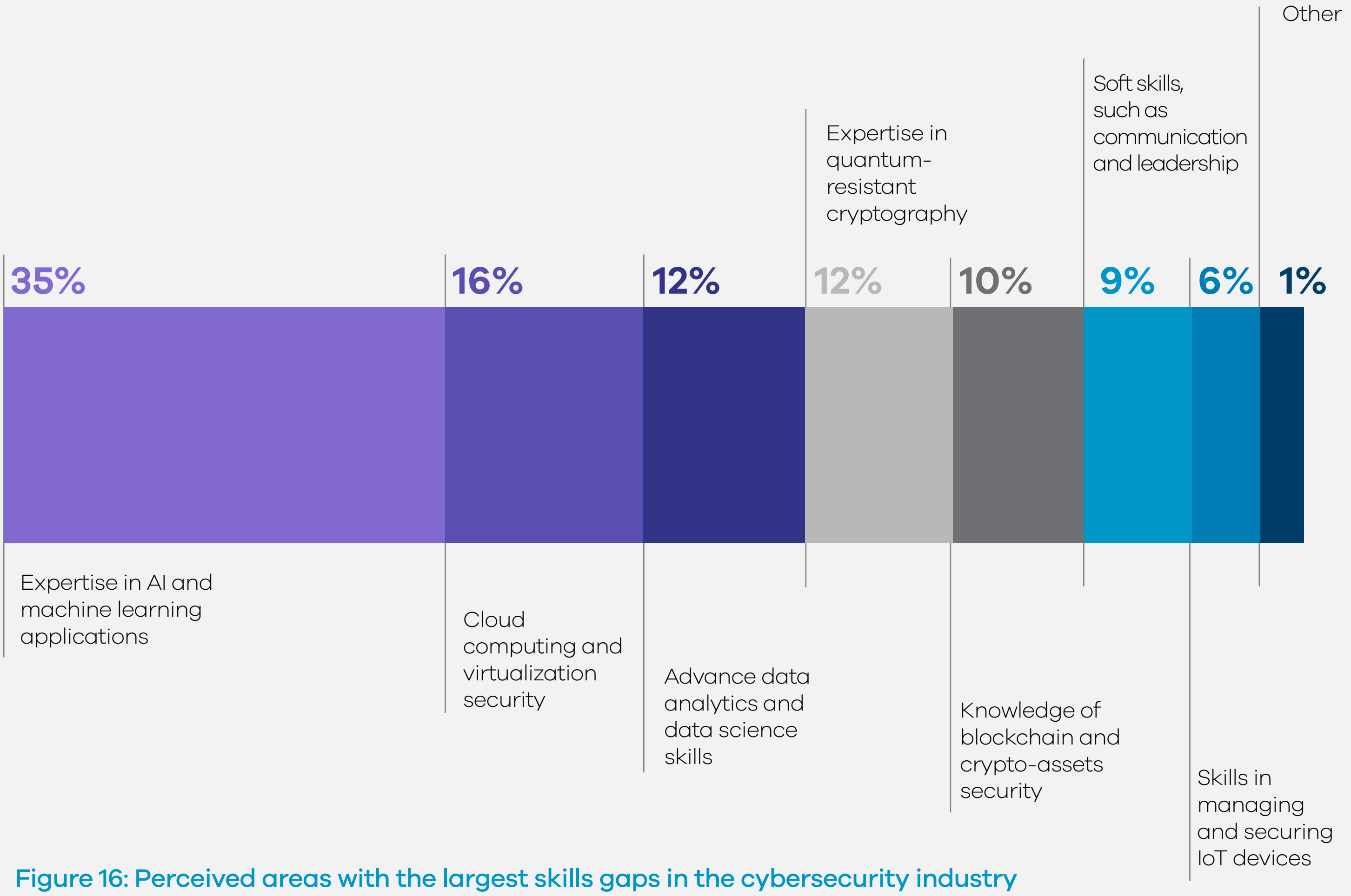


Figure 16: Perceived areas with the largest skills gaps in the cybersecurity industry

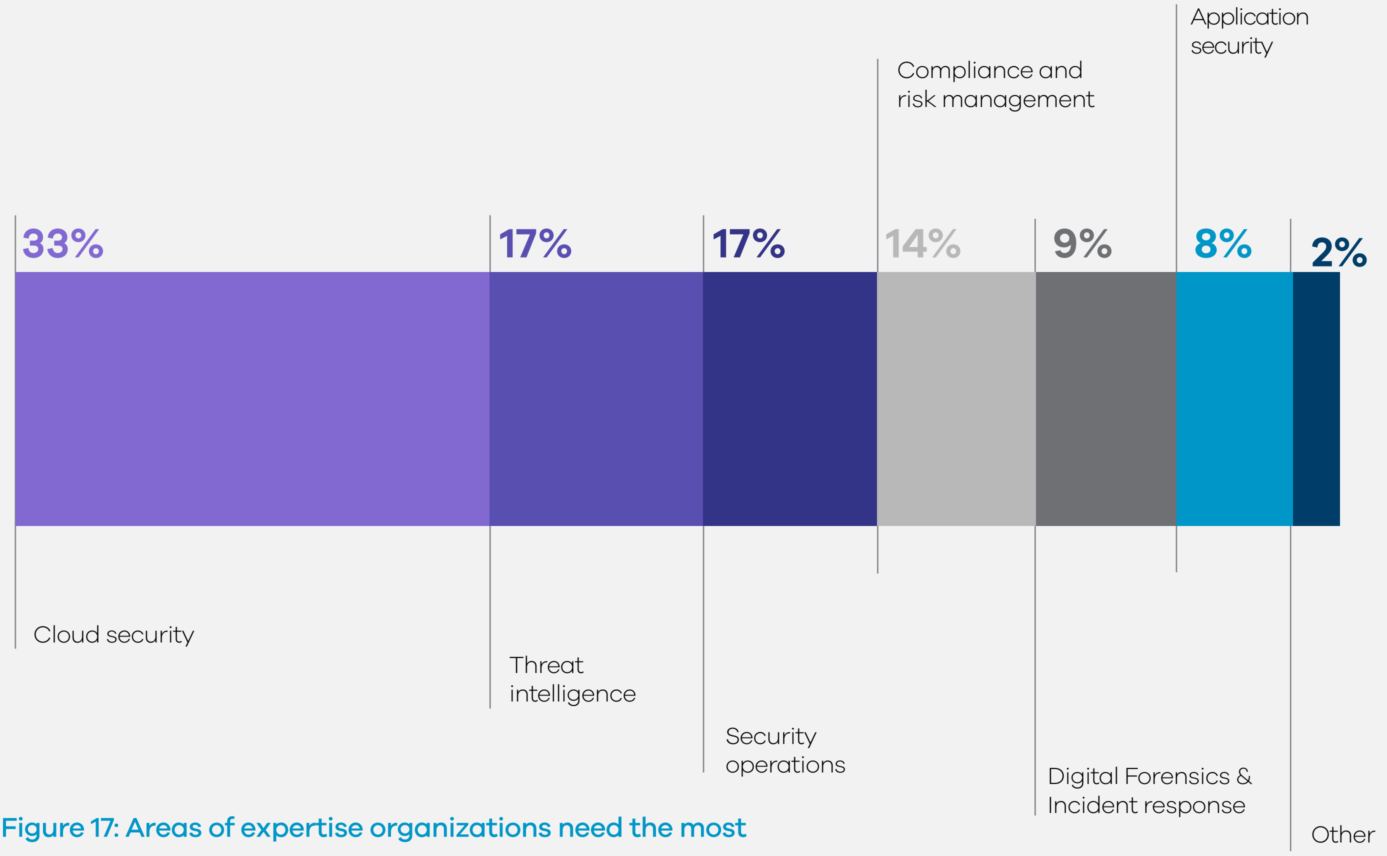


Figure 17: Areas of expertise organizations need the most

**Outlining the drivers of increasing demand and the actions that can be taken to bridge the gaps helps us better understand the workforce shortage and skills gap.**

### 5.1.1 Factors fueling cybersecurity workforce challenges

Challenges impacting the preparedness of the cybersecurity workforce are driven by both external and internal organizational factors, and contribute to both workforce shortages and skills gaps, as outlined below.

#### External factors

- **Fifth domain:** In 2011, the U.S. Defense Department designated Cyberspace the fifth operational domain, alongside land, sea, air, and space. NATO acknowledged this in 2016. Since then, the demand for a cyber workforce has significantly increased.

- **Cyber-physical integration:** The integration of cyber-physical systems (CPS) in various sectors, including manufacturing, healthcare, transportation, and critical infrastructure, has significantly heightened the need for specialized security skills. CPS involves the convergence of physical and digital worlds, creating highly complex systems that require expertise in both domains. Traditional cybersecurity skills must be improved; professionals must understand the physical processes and the corresponding cyber components. Threats to CPS are often more sophisticated, involving both cyber and physical elements. Defending against these requires advanced knowledge in both areas, thus demanding higher skill levels.

- **Ever-changing cyber threat landscape:** Attackers using advanced techniques such as polymorphic malware, zero-day exploits, and multi-vector attacks have begun leveraging the power of AI more to evade traditional security measures. These sophisticated methods require equally sophisticated defense mechanisms and a deep understanding of emerging threats. Cybercriminals increasingly focus on targeted attacks, such as spear-phishing and advanced persistent threats (APTs). These attacks are often well-researched and specifically tailored to exploit vulnerabilities in a particular organization or individual, making them harder to detect and prevent.

- **Increasing focus on sovereignty in critical areas of cybersecurity:** Given the present geopolitical climate, governments all over the world have been boosting investments into their R&D capability within critical information systems, including defense, national security, cryptography, communications security, data security, AI security, cyber intelligence, secure software development, etc. This investment is seen as crucial for reducing reliance on supply chains that cannot be controlled in a sufficiently sovereign manner, understanding and mitigating the APTs in real-time independently of foreign third parties, and fostering sovereign innovation to propel long-term economic growth.

- **Cybercrime as a well-funded commercial vertical:** Cybercrime operates through highly organized and sophisticated networks. Dark web markets facilitate the sale of stolen data, malware, and other illegal services. Profits are substantial, with cybercriminals generating billions of dollars annually. While revenue is difficult to quantify directly, the cost of cybercrime indirectly estimates the income cybercriminals generate. According to analysis by the Boston Consulting Group (BCG), the global price of cybercrime increased from $445 billion in 2014 to $2.2 trillion today.[1] In 2023, the reported revenue generated by ransomware payments exceeded $1 billion.[12] Fund allocation for cybercrime activities is much cleaner and less methodical than enterprise budget planning, providing attackers with an asymmetric advantage compared to their target counterparts.

### Internal factors

- **Asymmetric game:** Defending modern organizations is becoming increasingly complex. Modern IT environments often involve hybrid cloud infrastructures, cyber-physical systems, remote work setups, and a multitude of interconnected systems and applications, including IoT and mobile devices. This has exponentially increased an organization's attack surface, where each connected device and service represents a potential entry point for attackers. Simultaneously, organizations must also navigate an increasingly complex and demanding landscape of regulations and compliance requirements related to data protection and cybersecurity.

- **Cyber talent challenge:** Attracting and retaining cybersecurity talent presents significant challenges. Inadequate compensation remains a primary issue, with 54% of organizations identifying it as a major barrier. Moreover, there is a limited talent pool, according to 49% of respondents. This dual challenge indicates that organizations must design attractive career paths and competitive compensation packages to successfully attract and retain skilled cybersecurity specialists.

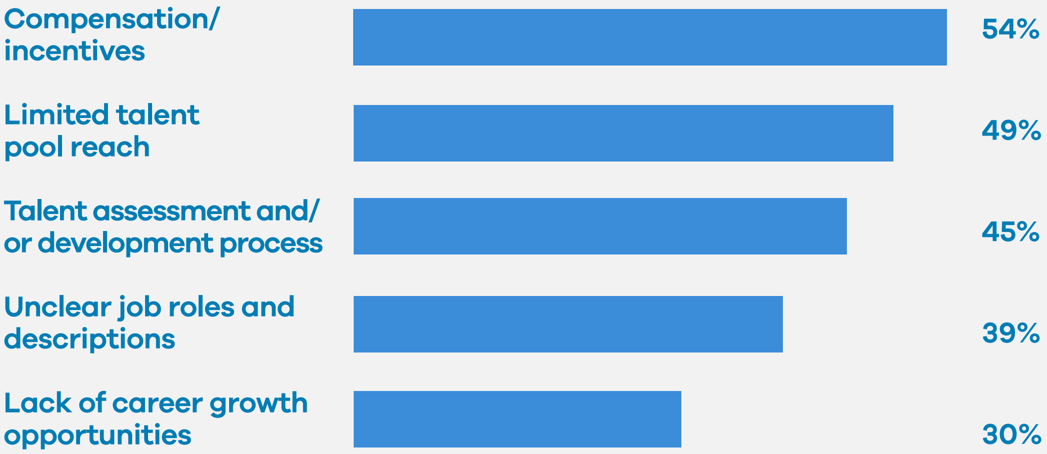
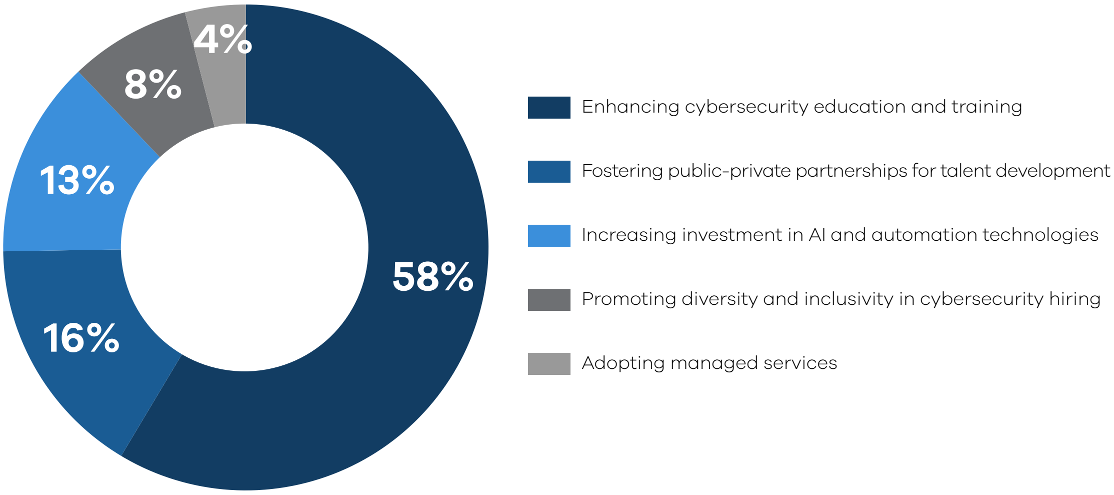


Figure 18: Challenges in attracting and/or maintaining cybersecurity talent

## 5.2 Opportunities for organizations to tackle workforce challenges

**Addressing the cybersecurity workforce shortage and skills gap requires coordinated efforts across education, industry, and government.**

By enhancing educational programs, promoting continuous learning, and leveraging technology, organizations can develop a workforce capable of meeting current and future security challenges. Although there is no one-size-fits-all solution, our research indicates that the best approach for organizations to address the skills gap and develop talent is through training the existing workforce, fostering public-private partnerships, and investing in AI.



Note: Numbers might not sum up to 100 due to rounding

Figure 19: Strategies that should be prioritized to address the cybersecurity skills gap

### 5.2.1 Education and training

**Research findings highlight the importance of both external and internal training in addressing the skills gap.**

External training helps organizations gain new skills, while internal training scales skills across the organization. As shown in Figure 20, organizations plan to address the skills gap primarily through internal training and development programs, partnering with educational institutions, and hiring external consultants and experts.

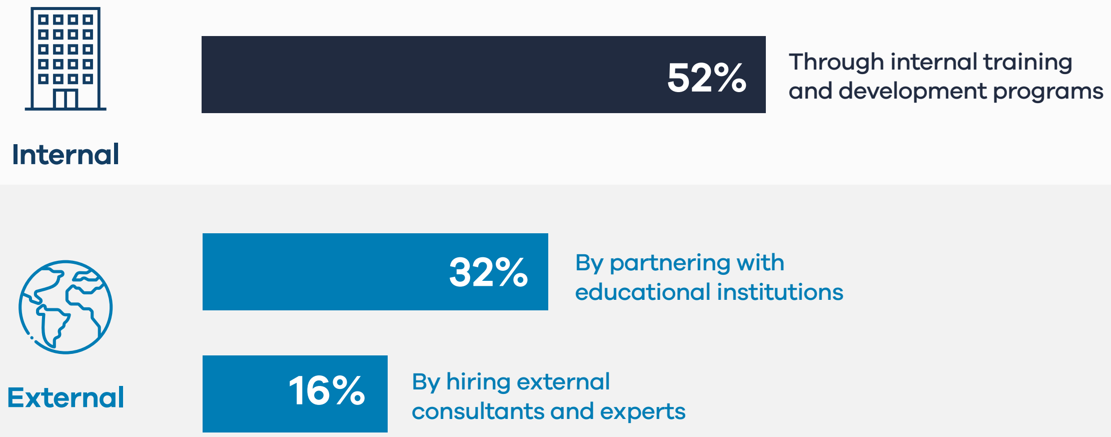


Figure 20: How organizations plan to address the cybersecurity skills gap in the long term

## Several other best practices can be implemented to reduce the skills gap and workforce shortage:

- **Experiential training and education:** The educational landscape is experiencing an e-learning revolution driven by experiential learning. This shift has been made possible by advancing and adopting cloud technology, infrastructure-as-a-service, container technology, attack simulation solutions, and threat emulation solutions. Experiential learning emphasizes hands-on, practical experience, allowing learners to apply theoretical knowledge in real-world scenarios. For instance, cyber drills provide immersive experiences, enhancing skills and readiness for actual threats. Looking ahead, we can expect further integration of AI and machine learning to personalize and improve the effectiveness of experiential learning.

- **Improved access to security education:** Cybersecurity education and training have traditionally been delivered through face-to-face, instructor-led activities, which have proven costly and not equally accessible across different demographics and organizations, depending on available and allocated training budgets. The maturity of cloud technology in recent years has fostered the development of numerous business-to-consumer (B2C) self-paced training providers, making access to cybersecurity training and education much more widespread.

- **Cyber range technology and solutions:** Once largely confined to the military and research domains, cyber range technology and solutions have become widespread and are expected to reach a strong level of maturity in the next two to three years. This will facilitate independent and self-paced experiential learning, previously available through in-person training.

- **Continuous Professional and Experience Development (CPED):** Traditionally referred to as Continuous Professional Development (CPD), this is a process through which professionals continue their upskilling, usually through self-reporting of learning (e.g., a new certification achieved or seminars attended) and experience activities (e.g., development and delivery of workshops, conference talks). As experimental content and cyber range solutions become more mainstream and accessible, professionals can add continuous practical experience to their profile, which can be more easily validated compared to the current self-declaration approach.

### 5.2.2 Public-private partnerships

**Public-private partnerships are essential for bridging the workforce shortage and the skills gap as they combine resources and expertise to create robust workforce development programs.**

These collaborations enable targeted training initiatives for diverse demographics, expanding the talent pool and providing specialized courses and conferences for continuous skill enhancement and preparedness for evolving industry demands.

- **Research and Development (R&D) capability-building programs:** As major governmental and private entities mature and build their internal, expert-driven (R&D) departments, vendors have offered dedicated, comprehensive Transfer-of-Knowledge programs to address this increasing demand. At one end of the spectrum, individual employees attend specialized online courses and hybrid international conferences on selected topics, or enroll in graduate and post-graduate educational programs at major universities. At the other end, R&D departments invest in customizing advanced capability-building programs and sovereign technology development for units dealing with the most security-critical topics, where the entire unit's staff is dedicated to the capability-building program part-time over a prolonged period.
- **Workforce development activities:** Governments have begun allocating funds to foster the development of workforce initiatives across affected demographics, including defense/government personnel exiting service and financially disadvantaged communities, to cast a wider net and attract a new workforce to join the cybersecurity domain.

### 5.2.3 Artificial intelligence

**AI is expected to significantly improve human productivity, reduce human errors, and enhance job performance to secure future infrastructures and ecosystems.**

Figure 21 shows that 54% of organizations are considering acquiring an AI agent to help mitigate the skills gap, although 33% are not considering it in the near future; a smaller percentage remains undecided. However, over the last year, nearly every vendor in the security industry has introduced AI into their datasheet or roadmap and uses AI as a marketing tool to increase sales and product adoption.

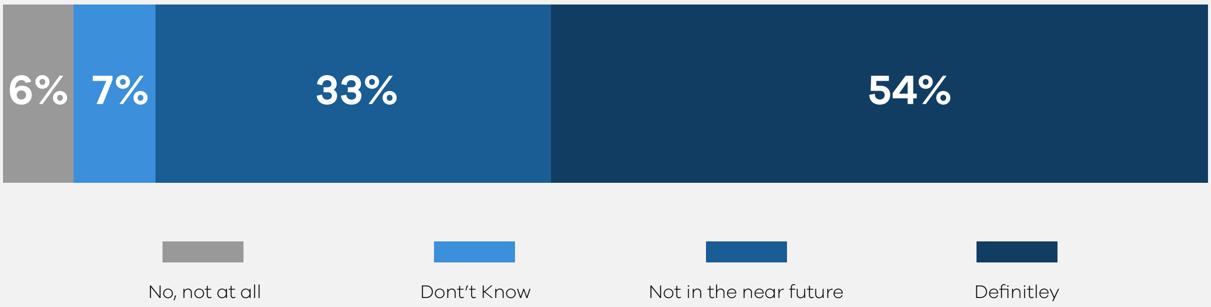


Figure 21: Organizations ready to acquire an AI agent to help mitigate the skills gap

While it may be too early to measure the value introduced by AI fully, it is expected that it will help close the skills gap, not only through performance improvements, but also by advancing security education and training, which is considered the most effective approach for closing the skills gap, as depicted in Figure 19.

AI is expected to introduce major improvements in several areas of training and education. Three areas in particular can be identified:

- **Adaptive training and education:** AI-powered systems can tailor educational content to meet the individual needs of learners. AI can recommend customized study plans and experiential resources by analyzing learners' strengths, weaknesses, and learning pace, ensuring a more efficient learning process. New platforms will use AI to adapt content dynamically based on the learner's progress and performance, adjusting the difficulty level of tasks, introducing new topics when the learner is ready, and reviewing areas where the learner struggles. Adaptive training will also improve, using intelligent tutoring systems, which can provide human-like assistance to learners during their learning journey while adapting the learning experience based on the help requested.

- **Creation of realistic simulation environments:** AI-driven simulations and virtual environments can provide immersive training experiences. For example, in cybersecurity training, AI can create realistic scenarios of cyberattacks, allowing learners to practice and develop their skills in a controlled, risk-free environment. Creating such environments currently relies heavily on instructional content developers and could be faster and more flexible. AI can dynamically create content to provide adaptive learning and assessment activities.

- **Assessment:** AI will increasingly assess real human abilities beyond the dominant knowledge-based assessment system. As the ability to dynamically create content with AI increases, assessments will become more experimental and based on the practical abilities of individuals mapped to specific job roles. AI is also expected to improve current proctored assessment solutions by automatically detecting facial expressions and behavior to flag potential cheating or behavioral anomalies. AI can analyze the behavior of learners to predict potential security breaches or issues.

Major changes are expected in intelligent tutoring systems, where AI-powered systems will replace traditional static and hint-based tutoring solutions. However, the major developments and breakthroughs impacting the cybersecurity skills gap will be in the acceleration and automation of content creation. This is likely to happen in two phases, content acceleration and simulation tailoring:

- **Content acceleration:** This will involve developing AI-assisted content creation solutions where content creators and instructional designers can use AI to create baseline content that can be reviewed, edited, and configured. Content creation is currently a major bottleneck and cost center, especially for experimental content and the development of the network, user, and attack simulations. This process is presently fundamentally manual. As AI evolves, it will be possible to interact with an AI-instructional design app to automatically create experimental content such as virtual machines with specific vulnerabilities, background traffic, user emulation with specific profiles, or even attacks to emulate particular threat actors, up to eventually producing entire complex infrastructures and simulations. AI is expected to do the heavy lifting in creating and configuring baseline environments.
- **Simulation tailoring:** Once AI is mature enough to support the human-led content creation process, simulation tailoring will begin. AI will also be able to create simulation environments and emulations dynamically adapted automatically and more accurately to user profiles, capabilities, and goals.

Content acceleration is expected to mature within three years, enabling a more efficient content creation process. Simulation tailoring will likely follow, maturing within the next three to five years. Various business solutions will be developed and made available in the market during this time.

**Time to:**

**2-3 years**

**Content acceleration**

**3-5 years**

**Simulation tailoring**

Overall, as emerging technologies continue to evolve and become mainstream, it is clear that the future generation of cybersecurity professionals will need to possess competencies spanning across the Information and Communication Technology (ICT) and Operational Technology (OT) domains. Over time, these professionals will mature into more decision-making roles as AI-power systems and security solutions will gradually take over the execution of manual and repetitive tasks. Consequently, leadership roles will evolve to provide direction and resources, supporting effective digital transformation while maintaining accountability for the organization's risk exposure.

## 5.3 Top workforce trends in 2025

**Countries are substantially addressing the cybersecurity workforce gap through well-defined interventions.**

These efforts focus on three key actions: introducing cybersecurity workforce frameworks, scaling the domestic talent pipeline, and creating detailed cyber curricula and educator training programs.

### Introduction of cybersecurity workforce frameworks

Introducing and detailing cybersecurity workforce frameworks is a fundamental step in addressing the skills gap. These frameworks clarify the variety of job roles available within the industry and outline clear progression pathways for cybersecurity professionals to explore various career paths. This approach aims to improve transparency and systematically address the skills gaps in the cybersecurity sector. By establishing structured frameworks, nations can ensure individuals have clear career paths within cybersecurity fields.

Countries such as Australia, Saudi Arabia, Singapore, the US, and the United Kingdom (UK) have developed comprehensive Cybersecurity Career Frameworks. These frameworks provide an overview of the skills and competencies required at various levels, from entry-level positions to advanced specialist roles. They also highlight the necessary certifications, training, and experience for progression, offering a roadmap for individuals aspiring to enter or advance in cybersecurity. This structured approach enhances career development and ensures a consistent supply of qualified professionals to meet the growing demand in the cybersecurity industry.

### Scaling the domestic talent pipeline

Another critical action is scaling the domestic talent pipeline through dedicated training programs, scholarships and public-sector employment schemes. Countries are now investing in various educational programs, from military cyber education to specialized cyber curricula, to identify, train, and retain talent within their borders. China, Saudi Arabia, the US and the UK have initiated cyber academies and allocated funds to nurture cybersecurity experts. Some countries are also working on dedicated workforce strategies that aim to improve cybersecurity education and make it more accessible, encouraging a diverse range of individuals to pursue careers in this critical sector.

To further strengthen their cybersecurity workforces, countries such as Australia have established immigration incentives to attract foreign skilled workers and prevent the loss of domestic talent. Public sector employment schemes play a crucial role by offering competitive salaries, benefits, and opportunities for career advancement, helping to retain and grow the number of skilled professionals within the country.

### Creation of detailed cyber curricula and educator training programs

The final strategic shift involves creating detailed cyber curricula and comprehensive training programs for educators. By doing so, countries aim to build a solid foundation for long-term cybersecurity education and workforce development. Examples include the Detailed Cyber Curricula in the UK[13], the Cyber Educators Scheme in Singapore[14], the National Centers of Academic Excellence in Cybersecurity programs in the USA[15], and the SCyber-Edu framework in Saudi Arabia[16]. These programs focus on integrating cybersecurity education into the broader academic curriculum, from primary to higher education levels, ensuring that students are exposed to cybersecurity concepts early and are better prepared for advanced studies and careers.

Equally important are educator training programs. Students can receive up-to-date and relevant training if countries can work to equip teachers with the necessary knowledge and skills to deliver high-quality cybersecurity education. These programs can include professional development opportunities, resources, and support networks for educators, helping them stay current with the latest trends and technologies in cybersecurity.

# Conclusion

**Technological advancements present significant opportunities to enhance cybersecurity measures, improving detection and response capabilities. However, the rapid pace of innovation also introduces new vulnerabilities and sophisticated cyber threats.**

To address these challenges, organizations must adopt a proactive approach that allows them to monitor, understand, strategize, and transform their cybersecurity practices. By staying ahead of emerging threats and integrating new solutions effectively, organizations can maximize the benefits of technological advancements while mitigating associated risks.

Diverse and evolving global cybersecurity regulations create compliance challenges for multinational corporations. Nevertheless, these challenges also present opportunities for international cooperation to create a cohesive regulatory environment. Countries can simplify compliance and enhance global security by focusing on international collaboration and harmonizing cybersecurity regulations.

The cybersecurity workforce shortage and skills gap remain a significant concern. Investing in continuous learning and development programs is essential to close this gap and foster a more skilled and prepared workforce. Solutions include developing robust training programs, improving access to security education, and promoting public-private partnerships. Addressing the workforce and skills shortage through these initiatives is critical to ensuring that the cybersecurity workforce can be better equipped to meet current and future demands.

**Responding to opportunities and challenges in technology, geopolitics, and human capital through proactive strategies, international collaboration, and workforce development is essential for building a resilient cybersecurity posture. By embracing these solutions, stakeholders can navigate the complex and dynamic cybersecurity landscape, ensuring a secure Cyberspace and prosperous future.**

# Endnotes

1. Global Cybersecurity Forum and Boston Consulting Group (2024). 2024 Cybersecurity Workforce Report: Bridging the Workforce Shortage and Skills Gap. https://gcforum.org/en/research-publications/cybersecurity-workforce-report-bridging-the-workforce-shortage-and-skills-gap/

2. Global Cybersecurity Forum (2024). Navigating GenAI Threats and Opportunities in Cybersecurity. https://gcforum.org/en/research-publications/navigating-genai-threats-and-opportunities-in-cybersecurity-whitepaper/

3. Innov-acts (2023). The Impact of Generative AI on Cybersecurity: Opportunity or Challenge? https://innov-acts.com/the-impact-of-generative-ai-on-cybersecurity-opportunity-or-challenge/

4. Statista (2023). Number of Internet of Things (IoT) connections worldwide from 2022 to 2023, with forecasts from 2024 to 2033. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

5. Tom Gregory (2024). Certainty in the trajectory of patents for quantum computing. Appleyard Lees. https://www.appleyardlees.com/certainty-in-the-trajectory-of-patents-for-quantum-computing/

6. Official Journal of the European Union (2016). General Data Protection Regulation. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

7. Department of Health and Human Services (2024). The HIPAA Privacy Rule. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

8. Federal Trade Commission (2024). Gramm-Leach-Bliley Act. https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

9. Office of the Attorney General (2024). California Consumer Privacy Act (CCPA). https://oag.ca.gov/privacy/ccpa

10. Global Cybersecurity Forum (2024). Who We Are. https://gcforum.org/en/about/

11. Centre for Cybersecurity – World Economic Forum (2024). Centre for Cybersecurity. https://centres.weforum.org/centre-for-cybersecurity/home

12. Chainalysis (2024). Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline. https://www.chainalysis.com/blog/ransomware-2024/

13. GOV.UK (2017). Guidance: Cyber Schools Programme. https://www.gov.uk/guidance/cyber-schools-programme

14. CSR Singapore (2020). SG Cyber Educators. https://www.csa.gov.sg/our-programmes/talents-skills-development/sg-cyber-talent/sg-cyber-educators

15. National Security Agency (2024). National Centers of Academic Excellence in Cybersecurity. https://www.nsa.gov/Academics/Centers-of-Academic-Excellence

16. National Cybersecurity Authority (2020). The Saudi Cybersecurity Higher Education Framework (SCyber-Edu – 1: 2020). https://nca.gov.sa/ar/scyberedu_en.pdf

GLOBAL
CYBERSECURITY
FORUM

Site