CYBERSECURITY FRONTIERS:

A Perspective on Securing the Future of Cyberspace

Insight Report

April 2025

GLOBAL CYBERSECURITY FORUM | Site

Chairman's Message

Dr. Hesham Altaleb
Chairman, Future of Cybersecurity
Knowledge Community
Saudi Information Technology
Company - SITE

As technological advancements continue to accelerate at an unprecedented pace, cybersecurity has become an essential priority for organizations worldwide. In response to the growing sophistication of cyber threats and the expanding digital attack surface, organizations must adopt a proactive, intelligence-driven approach to cybersecurity. This report provides a forward-looking analysis of the cybersecurity landscape, identifying key emerging threats, technological shifts, and workforce challenges. It equips organizations with the knowledge needed to proactively address risks with actionable recommendations designed to strengthen defenses and harness the potential of emerging technologies.

The primary objectives of this report are twofold. Firstly, it seeks to enhance understanding of the future cybersecurity landscape. The report identifies emerging trends and potential risks by examining the dynamics of technological acceleration, international collaboration, and workforce transformations, offering a data-driven perspective that helps organizations stay ahead of emerging cyber threats.

Secondly, the report aims to deliver actionable recommendations. Recognizing the complexity and urgency of the cybersecurity challenges, it outlines strategic frameworks and practical guidelines. These recommendations are 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 to navigate the complexities of the cybersecurity landscape and supporting the creation of a secure and resilient future.

Leading 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)

Contents

Executive Summary

Cybersecurity is at a crossroads. The rapid adoption of artificial intelligence (AI), the Internet of Things (IoT), and 5G is transforming industries, unlocking new opportunities while simultaneously expanding the attack surface. As cyber threats grow in sophistication, resilience is no longer just about defense – it is a business priority. Organizations that fail to keep pace are at risk of operational disruptions, financial losses, and long-term vulnerabilities in an increasingly interconnected world.

The Future of Cybersecurity Knowledge Community survey at the center of this report highlights the urgency of this challenge. For instance, while nearly all respondents recognize cybersecurity as a competitive advantage, nearly as many acknowledge that emerging technologies are reshaping the threat landscape faster than organizations can adapt. The increasing complexity of cyber risks demands a proactive and structured response to ensure that businesses remain protected while continuing to innovate.

Technology alone will not close this gap. A severe global cybersecurity workforce shortage, compounded by economic pressures, rising salary expectations, and a complex training environment, threatens to undermine even the most advanced security solutions. Without enough skilled professionals to implement, manage, and refine security measures, organizations remain vulnerable despite technological advancements. Investing in workforce development, training, and cross-sector collaboration is essential to strengthening cyber resilience.

To help organizations navigate these challenges, this report introduces the MUST framework – **Monitor, Understand, Strategize, and Transform.** By continuously monitoring emerging threats and evolving technologies, organizations can gain a deeper understanding of their vulnerabilities and risk exposure. This knowledge enables them to develop targeted security strategies that align with business priorities, ensuring they invest in the right solutions and talent. The final step is transformation; leveraging AI-driven defenses, automation, and hands-on workforce development to build a future-ready security posture.

Cybersecurity is no longer just about safeguarding systems; it is about enabling innovation securely. Organizations that take a structured, forward-looking approach will not only strengthen their defenses but also position themselves for long-term success. By embracing these principles, investing in cybersecurity talent, and technology, businesses can build resilience, mitigate risk, and secure their Cyberspace.

1. Introduction

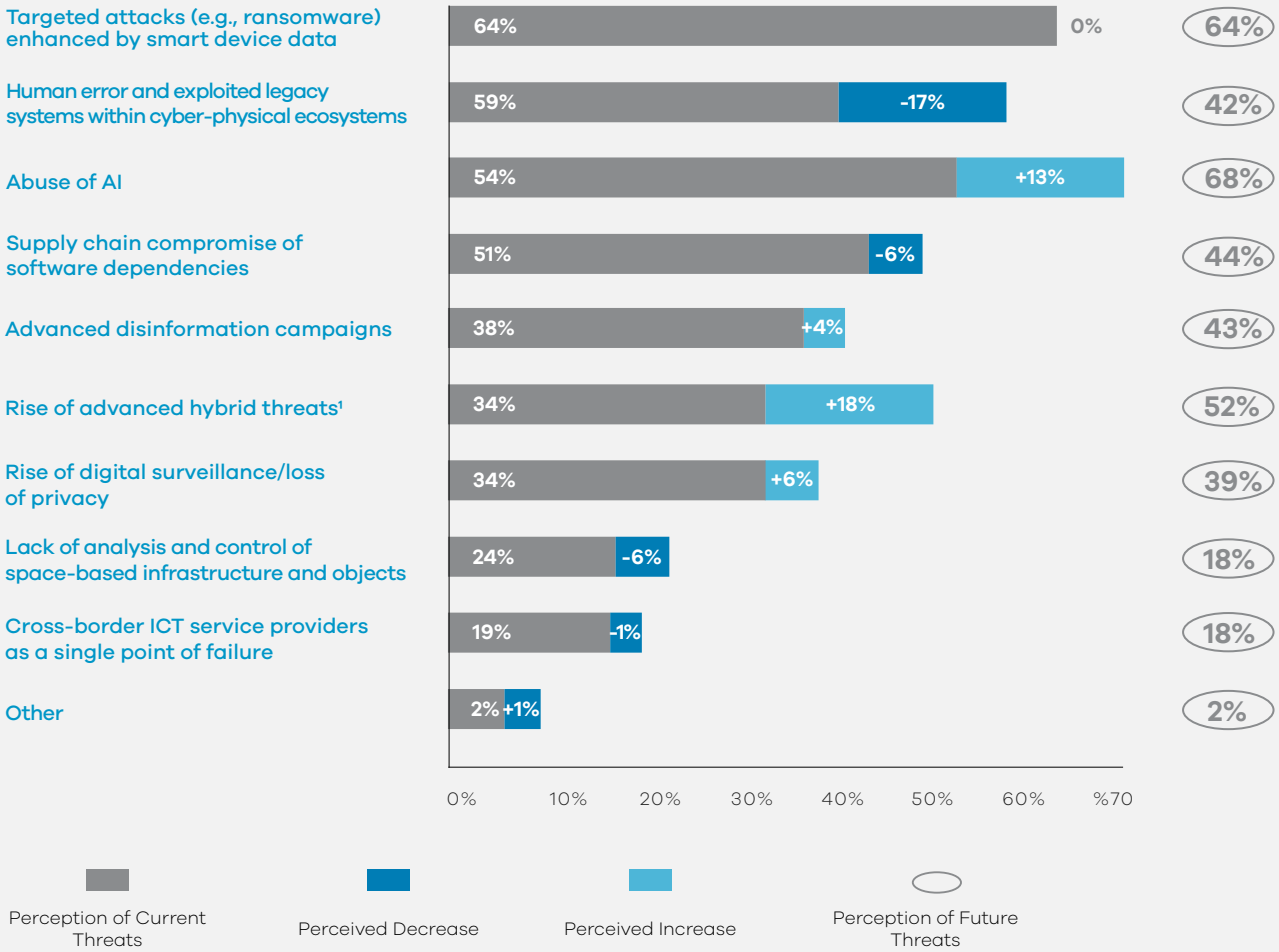
As the world undergoes a rapid and unprecedented technological revolution, the attack surface has expanded. Consequently, it has become essential for cybersecurity to evolve to safeguard society from potential disruptions caused by these threats. Additionally, the swift advancement of technological innovation is exacerbating the cybersecurity workforce shortage, with the demand for new skills surpassing the supply. This situation increasingly complicates the ability of organizations to train and recruit skilled professionals who can effectively navigate the complex landscape of modern cyber threats.

Building on the awareness of these critical challenges, this report addresses two interconnected elements vital to shaping the future of cybersecurity: technology and workforce transformation. Together, these two forces will define the effectiveness of future cybersecurity strategies—while emerging technologies offer new tools for defense, their successful adoption hinges on a skilled workforce capable of implementing and managing them. The report analyzes the evolution of cybersecurity through these two perspectives, providing valuable insights for professionals and decision-makers in the field while offering strategies to ensure strong protection in an ever more interconnected world.

2. Technological Acceleration

This selection 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.

Emerging technologies like AI, IoT, and quantum computing are shaping the future of technology while creating both opportunities and challenges for cybersecurity. According to our research, 68% of experts identify AI as a growing threat, 52% emphasize the rise of advanced threats, 39% highlight increasing data privacy concerns, and 43% point to the escalating impact of disinformation campaigns (Figure 1).



1. 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

Cybersecurity is therefore seen as a potential competitive advantage by an overwhelming majority of respondents. However, 86% believe organizations are not fully prepared to address future challenges (Figure 2). This highlights an urgent need for organizations to improve their vigilance and adaptability in cybersecurity strategies to remain competitive.

95%

Consider cybersecurity as a competitive advantage

86%

Think organizations are not fully prepared for future challenges

Figure 2: Survey participants understand the importance of cybersecurity but indicate that organizations are inadequately prepared for future cybersecurity challenges

To bridge this gap, organizations are turning to emerging technologies as a critical component of their cybersecurity strategies. Organizations are investing in emerging technologies, with AI for cybersecurity (89%), IoT security (52%), and secure 5G connectivity (36%) (Figure 3) under consideration or already being implemented.

However, some technologies have yet to demonstrate significant value in their adoption. For instance, quantum computing's nascency means it has yet to generate meaningful returns on investment. Similarly, blockchain projects are yet to yield significant returns on investment due to unclear value propositions and substantial implementation challenges. Our survey also reveals that investments in these technologies are limited by skills gaps (69%), the pace of technological innovation (56%), and integration with existing systems (53%). As a result, organizations opt to prioritize investments in technologies with proven benefits.

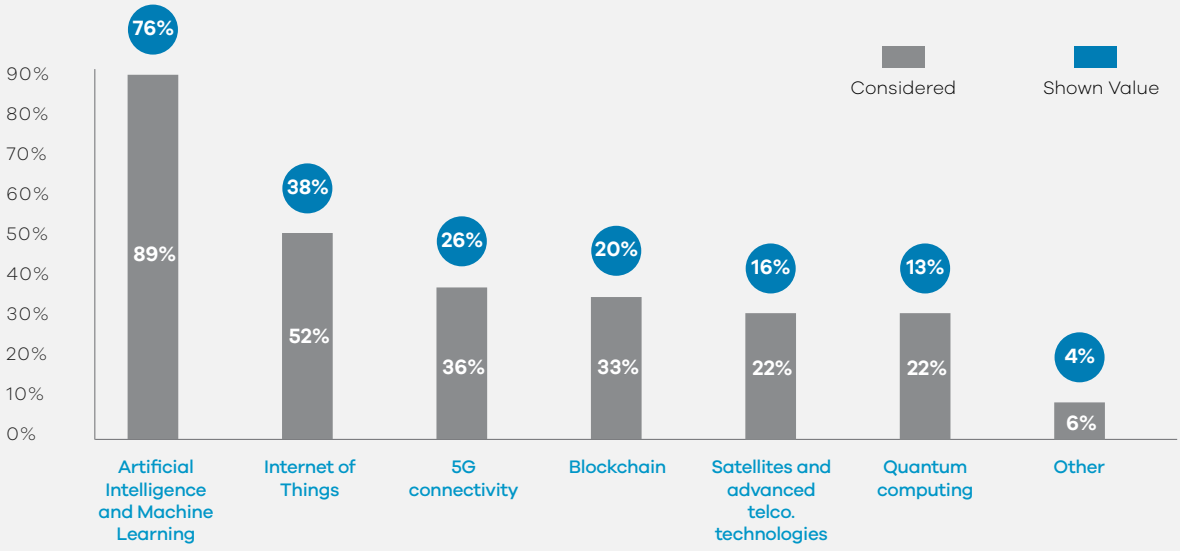


Figure 3: Organizations are prioritizing investments in emerging technologies that offer realizable value

2.1 Emerging Technologies in Cybersecurity

2.1.1 Transforming Cybersecurity with AI

AI's rapid growth has introduced both powerful tools for defense and evolving threats in cybersecurity. On one hand, AI enhances cybersecurity by automating threat detection and response, improving efficiency and accuracy. On the other, it enables more sophisticated cyberattacks, such as AI-generated phishing emails and malware that can bypass traditional security measures. This dual nature of AI means it benefits both cybersecurity defenders and malicious actors[1].

AI's role in cybersecurity offers significant advantages, including faster threat identification, reduced response times, and a stronger overall security posture. By automating routine security tasks, organizations can free up human experts to focus on more complex threats. AI's predictive capabilities also allow organizations to analyze patterns and anomalies in data, enabling proactive defense strategies. Given these benefits, it is unsurprising that 70% of organizations have integrated AI or generative AI into their cybersecurity operations[2].

However, AI also empowers attackers by making phishing campaigns more convincing, developing advanced malware, and automating entire cyberattack lifecycles. According to the survey, 54% of respondents currently recognize AI-related cybersecurity risks affecting organizations – a figure expected to rise to around 68% in the future (Figure 1). Additionally, AI systems are increasingly becoming targets of cyberattacks, highlighting the need for AI-specific security measures.

Recent data highlights the tangible nature of AI-related threats. Approximately 38% of organizations experienced at least one attack involving AI or generative AI-powered malicious code generation. The incidence is even higher for AI-embedded malware, which affected 59% of organizations, and for AI-enhanced automated phishing attacks, which impacted 72%[3].

As a revolutionary new technology, our research shows that AI is generally perceived positively, suggesting reliance on it for cyber defense will likely soon increase. However, as shown in Figure 4, opinions vary on its role in defense strategies. Enthusiasts (29%) believe it will be key to threat detection and response. The cautious majority (56%) view AI as supportive, focusing on specific tasks. Meanwhile, laggards (14%) have only begun experimenting with the technology, and skeptics (1%) believe it will not impact cybersecurity. Additionally, there are pertinent concerns regarding the use of AI in 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%). Taken together, these findings suggest that, as AI adoption in cybersecurity grows, organizations will need to adapt to an emerging array of challenges.

Figure 4: Attitudes toward the role of AI in cybersecurity defense strategies

2.1.2 Unlocking IoT's Potential While Preserving Security

As illustrated in Figure 3, IoT has been seen as the second most widely used emerging technology, after AI, indicating that the technology has already demonstrated significant value within their organizations. The future outlook for IoT is also promising, with the number of devices expected to increase dramatically, rising from 18 billion today to 39.6 billion by 2033[4].

However, as the number of connected devices grows, so will cyberattacks. Many IoT devices currently lack robust security features, rendering them vulnerable. IoT has also played a key role in converging information technology (IT) and operational technology (OT). As this continues, it could expose OT systems, which have traditionally remained isolated and secure from cyberattacks.

Results from our survey (Figure 5) suggest that organizations 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%) to address these threats.

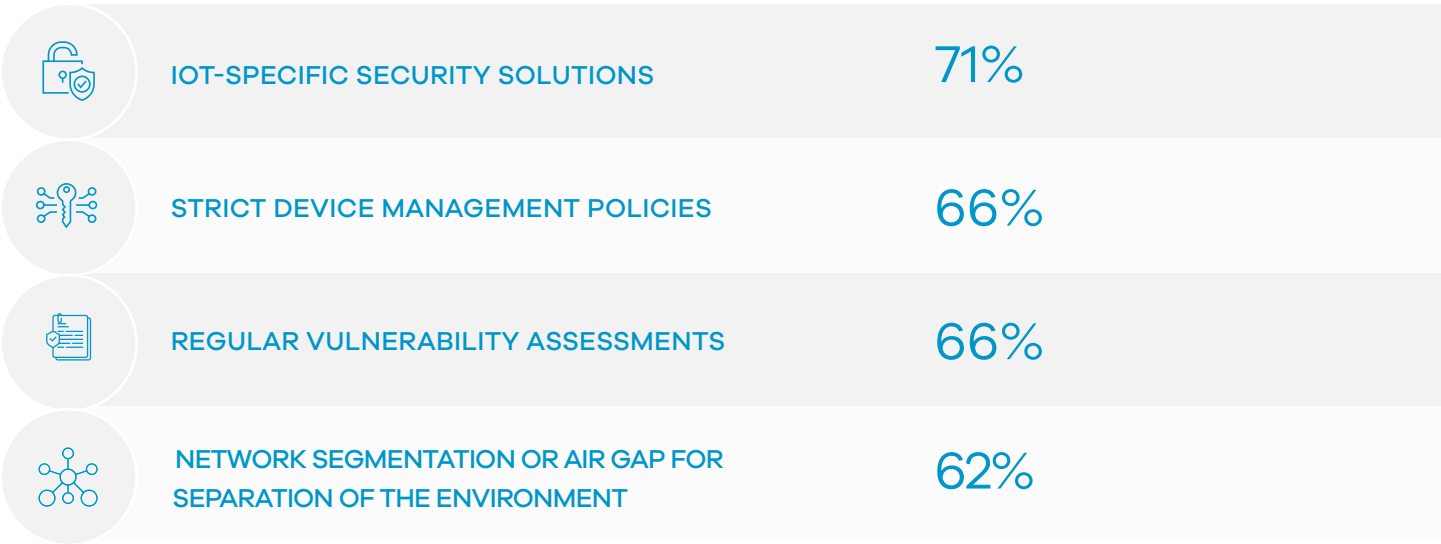


Figure 5: Suggested approach for IoT risk management

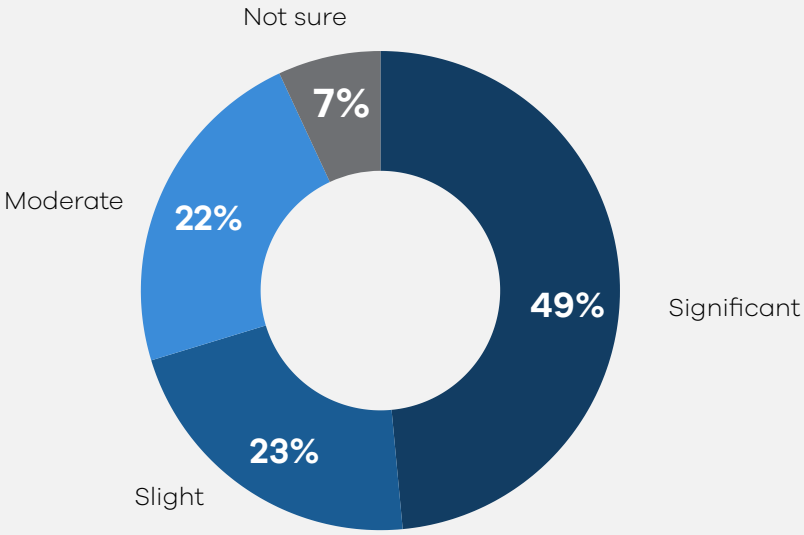
Additionally, the proliferation of smart home devices, often with minimal security, poses risks to individual privacy and safety; the delineation of responsibility for IoT security between consumers and businesses further complicates the issue. To enhance the security and privacy in smart home environments, consumers should follow several best practices. Connecting smart devices to a local network hub using protocols like Zigbee or Z-Wave is one effective strategy. These wireless protocols, specifically designed for smart devices, operate on a separate network from typical home Wi-Fi systems, adding a layer of security by isolating devices from direct internet exposure.

However, it is important to remember that this separation may not always be upheld, particularly with hubs that transmit data over the internet. Therefore, selecting trustworthy hubs is crucial. Additionally, some devices may require internet connectivity to function properly, even if they have local control options. In such cases, disconnecting from the internet could render the device inoperative. Being aware of these factors allows consumers to make informed choices, ensuring their smart home devices operate securely while maintaining their desired functionality.

2.1.3 Quantum Computing: An Opportunity and a Challenge

Although the development of a general-purpose quantum computer remains uncertain, most respondents (49%) believe that quantum computing will significantly impact encryption within the next five years (Figure 6).

This is unsurprising, given that research into and progress of this 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 6: Expected impact of quantum computing on encryption over the next five years

The development of quantum computers introduces the ability to harvest encrypted data now and decrypt it later. This highlights the importance of implementing quantum-safe cryptography before quantum computers are available to maintain long-term integrity and ensure ongoing security.

Survey respondents highlighted key strategies when asked how organizations should prepare for the anticipated impact of quantum advances on cybersecurity. The top recommendations include monitoring and planning for ongoing advancements (68%), collaborating with cybersecurity consortia to enhance quantum readiness (63%), and investing in quantum-resistant cryptography (47%) proactively.

Initial steps organizations can take include[6]:

1) Inventory all hardware, firmware, software, operating systems, and applications that use current encryption algorithms. Automated discovery tools can help here.

2) Prioritize the components that need to be migrated based on risk management methodologies that assess the sensitivity of the data and the potential impact of the attack. This will provide a roadmap for action.

3) Integrate and test new standards. Detailed instructions for incorporating the new tools into products and encryption systems should be tested to ensure they are functioning correctly and securely, without impacting performance negatively.

4) Train key security personnel and equip them for ongoing monitoring and updating. Collaborating with vendors to ensure new standards are adopted can help against attacks resulting from third-party software.

2.2. Cybersecurity Threat Landscape and Best Practices in 2025

As emerging technologies continue to evolve and reshape Cyberspace, it is important to prioritize threats and risks according to the severity and likelihood of occurrence.

Figure 7 ranks the cybersecurity threats that survey respondents are most concerned about for 2025.

The top three are:

1) AI-Powered Cyberattacks: (Gen)AI's ability to generate content (e.g., code) and automate part of the attack introduces new challenges in cybersecurity, requiring ongoing improvements in defensive strategies.

2) IoT Vulnerabilities: Many IoT devices lack robust security measures, making them easy targets for attackers to exploit.

3) 5G Network Threats: 5G's widespread adoption, due to its increased connectivity, makes networks more vulnerable to cyberattacks.

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

To address these and other evolving threats, the survey identified three best practices that can aid cybersecurity efforts in 2025 (Figure 8):

1) Zero Trust Network Access (ZTNA) is a security framework that operates on the principle of no inherent trust, requiring identity verification for all users and devices accessing resources. ZTNA is crucial as a response to evolving AI-powered cyber threats, as traditional perimeter security measures fall short. By enforcing continuous authentication and adapting access controls based on real-time risks, ZTNA provides necessary defense against AI's capacity to automate attacks and exploit vulnerabilities. Implementing AI-aware security policies within a Zero Trust model helps organizations combat both known and emerging threats.

2) 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.

3) 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.

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 8: Cybersecurity best practices for 2025

The threats and best practices identified demonstrate that cybersecurity professionals are aware of the challenges posed by increasingly sophisticated cyber threats. However, the onus is on organizations to be proactive and implement comprehensive security measures to safeguard critical assets and prevent potential attacks.

3. Workforce Transformation

In the rapidly evolving cybersecurity landscape, the importance of the human element cannot be overstated. While technological solutions are essential for defending against cyber threats, the ultimate effectiveness of cybersecurity relies on the individuals who design, implement, maintain, and operate those solutions. This section discusses the crucial role the cybersecurity workforce plays and the key challenges it is faced with.

Our survey (Figure 9) reveals that 95% of respondents feel that a transformation in the cybersecurity workforce is already underway. However, the causes attributed to this shift are varied and include the evolution of threats (76%), technological progress (71%), organizational demands (54%) and adherence to national cyber strategies (51%). These results suggest that workforce transformation varies greatly, significantly influenced by the specific context of an organization, including 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 9: Factors driving workforce transformation

3.1. Contextualizing Cybersecurity Workforce Challenges

The cybersecurity workforce faces a shortage of professionals, exacerbated by a widening skills gap. The workforce shortage refers to the difference between the demand for cybersecurity experts and their current availability. Recent data reveals a global shortage of 2.8 million professionals, representing about 39% of the existing cybersecurity workforce[2].

While increasing the number of professionals is important, continuously enhancing their skills is a key factor in keeping Cyberspace safe. The skills gap refers to the mismatch between the expertise organizations need and the talent available, both internally and externally.

Findings from our research underscore the scale and significance of the skills gap challenge (Figure 10); over 95% of respondents acknowledge a skills gap, with more than 42% asserting that it is significant.

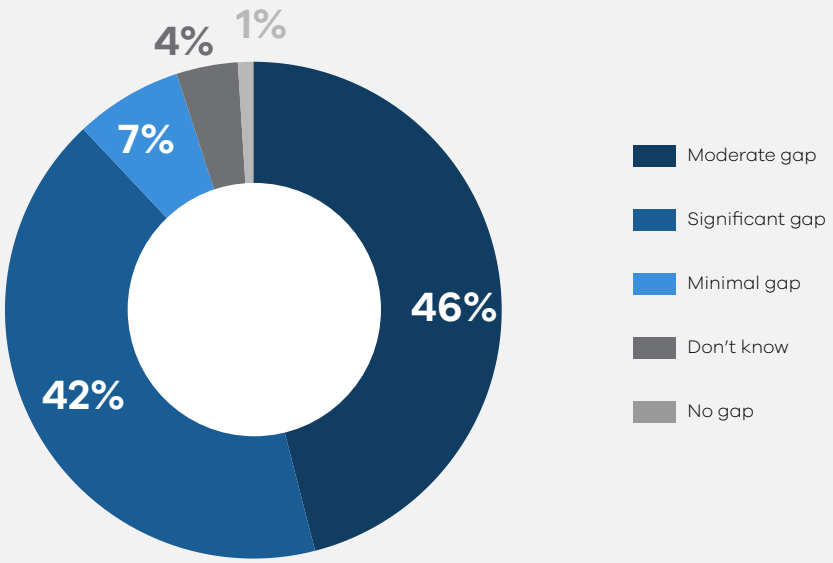


Figure 10: The current cybersecurity skills gap

As shown in Figures 11 and 12, the specific gap in skills and expertise varies significantly depending on the organizational context, complicating the possibility of a universal solution.

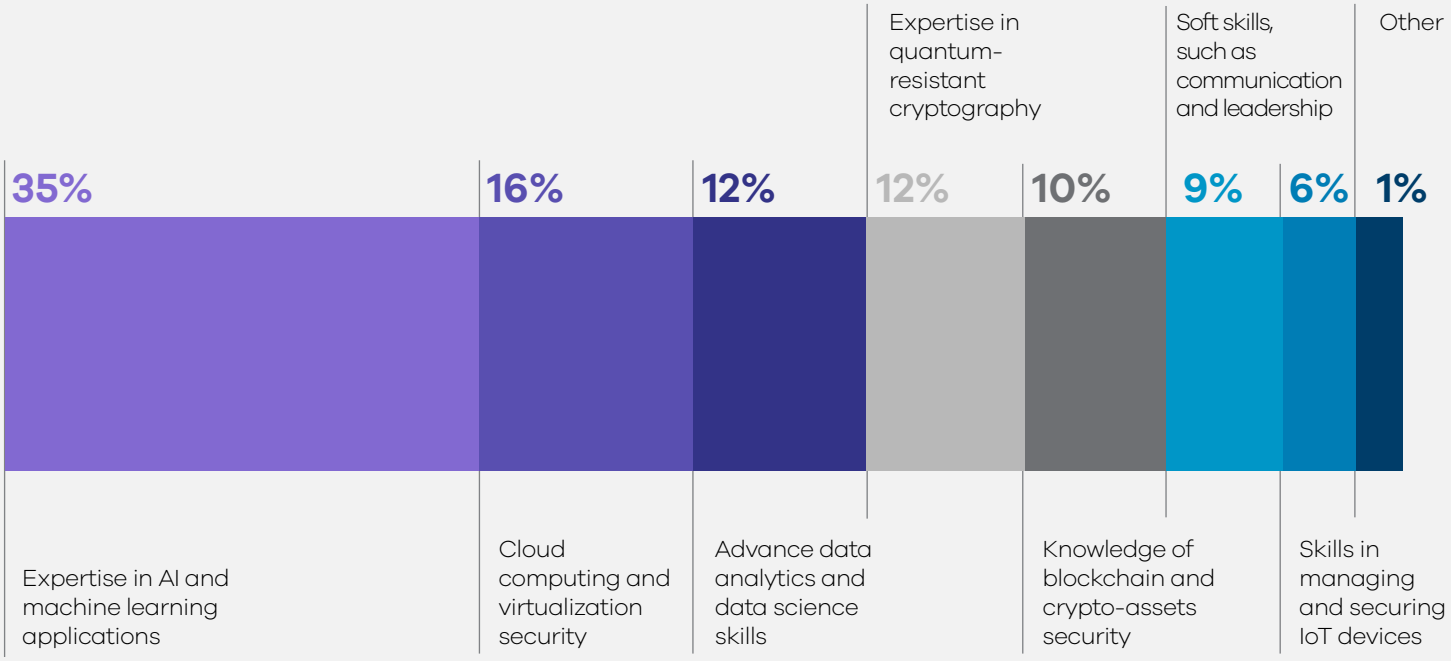


Figure 11: Perceived areas with the largest skills gaps in the cybersecurity industry

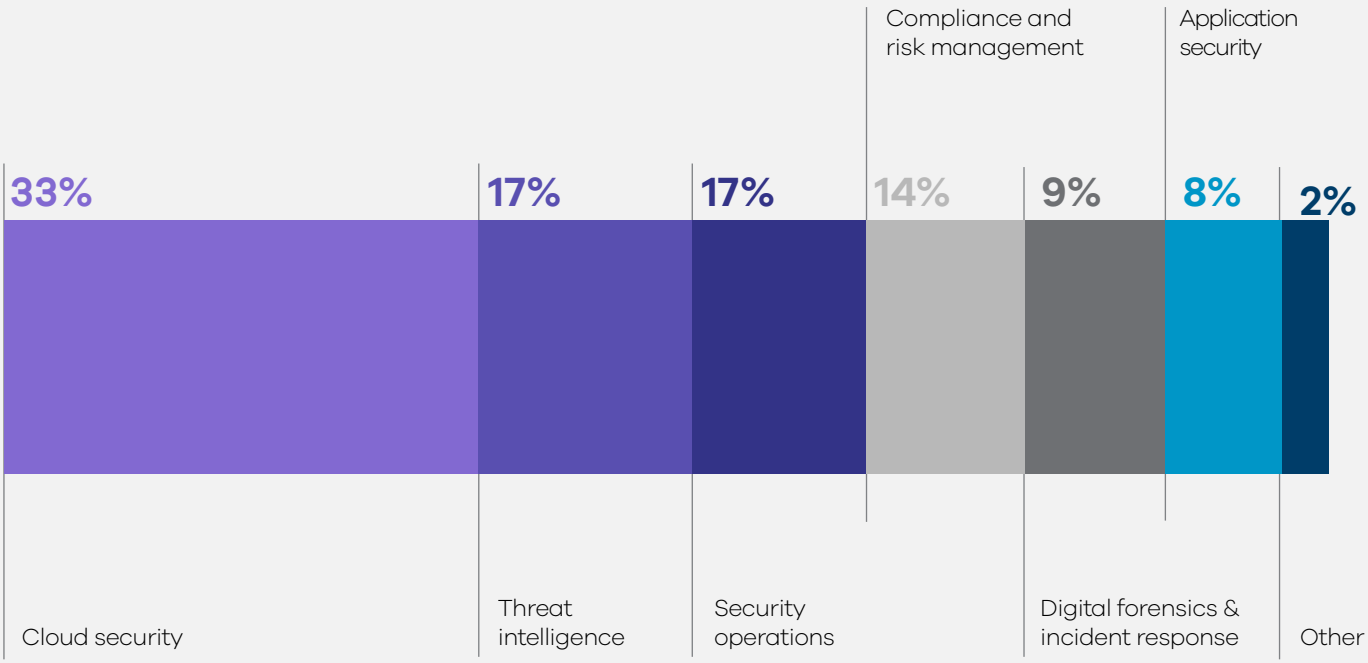


Figure 12: Areas of expertise organizations need the most

3.1.1 Factors Fueling the Cybersecurity Workforce Challenges

The challenges affecting the readiness of the cybersecurity workforce stem from various external and internal organizational factors, leading to workforce shortages and skills gaps, as detailed below.

External Factors

- **Fifth Operational Domain:** Cyberspace's classification as an operational domain for warfare, alongside land, sea, air, and space, has greatly increased investment in the industry and, consequently, the need for more specialists.
- **Cyber-Physical Integration:** Integrating cyber-physical systems (CPS) in healthcare, transportation, and critical infrastructure presents complex security challenges. Defending CPS necessitates expertise in both physical processes and digital technology to counter sophisticated threats, highlighting the need for non-traditional skills.
- **Localizing Cybersecurity Capabilities:** Governments are increasing their investments in cybersecurity research and development across areas such as secure systems, cryptography, AI security, and cyber intelligence.
- **Evolving cyber threat landscape:** Cyber threats are becoming more advanced, with attackers using new technologies and dark web networks to exploit vulnerabilities. This evolution requires highly skilled cybersecurity specialists who can adapt to these changes.

Internal Factors

- **Increasing Attack Surface:** Defending organizations is becoming increasingly complex. Modern IT environments include hybrid cloud infrastructures, cyber-physical systems, remote work setups, and many interconnected systems, such as IoT and mobile devices. Each connected device and service represents a potential entry point for attackers, significantly expanding an organization's attack surface.
- **Cyber Talent Challenge:** Talent acquisition and retention is a considerable challenge, with 54% of respondents citing insufficient compensation as a key problem, complicated by an already limited talent pool (Figure 13). Organizations must offer career pathways and competitive salaries to attract and retain skilled cybersecurity professionals effectively.

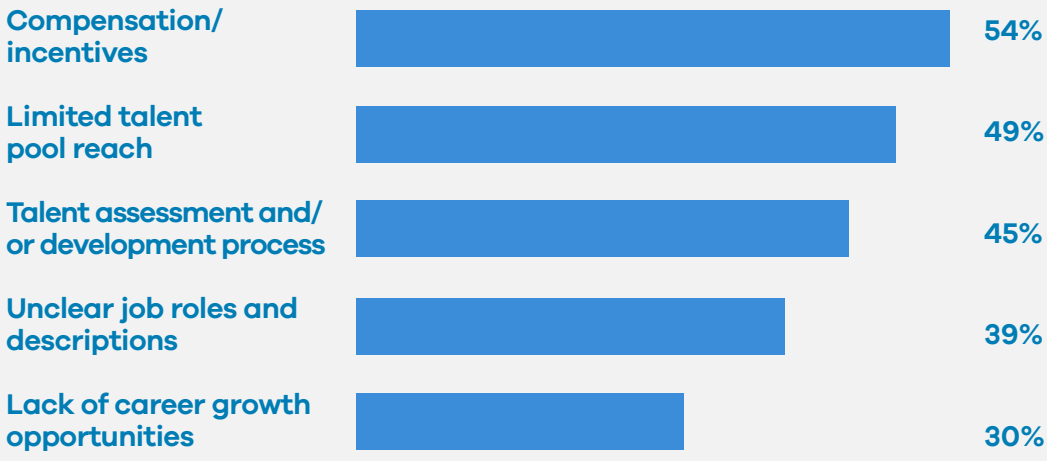
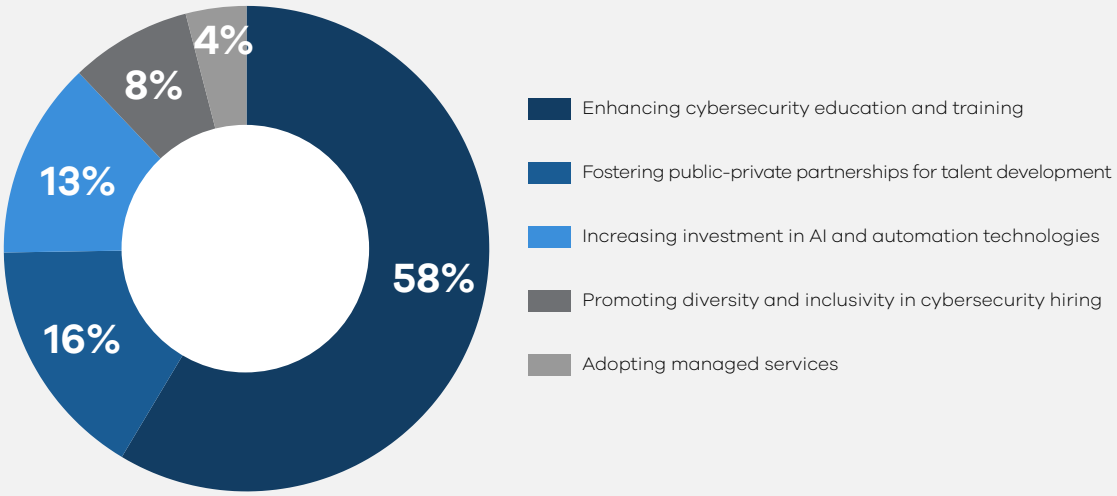


Figure 13: Challenges in attracting and/or maintaining cybersecurity talent

3.2 Opportunities for Organizations to Tackle the Cybersecurity Workforce Challenges

To tackle the shortage of cybersecurity professionals and the skills gap, organizations must cultivate a workforce equipped to handle both current and future security challenges.

While no universal remedy exists, organizations can effectively address the skills gap and nurture talent by training their existing workforce, encouraging public-private collaborations, and investing in AI technology (Figure 14)[7].



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

Figure 14: Strategies that should be prioritized to address the cybersecurity skills gap

3.2.1 Education and Training

As illustrated in Figure 15, the majority of organizations surveyed intend to address the skills gap through internal training and development programs, with the remaining opting for collaborations with educational institutions or hiring external consultants and experts.

However, a combination of external and internal training can play a more significant role in tackling skills gaps; external training enables organizations to acquire new skills, while internal training disseminates those skills throughout the organization.

Figure 15: How organizations plan to address the cybersecurity skills gap in the long term

Other ways organizations can reduce skills gaps and workforce shortages can involve:

- **Experiential Training and Education:** E-learning's growing emphasis on experiential learning involves hands-on training, allowing learners to apply theoretical knowledge to real-world situations. In cybersecurity, this could take the shape of immersive drills that simulate actual threats to test the skills and readiness of professionals. In the future, AI and machine learning will further personalize and enhance the effectiveness of experiential learning.

- **Improved Access to Security Education:** Traditional cybersecurity education and training have been delivered face-to-face, which can be costly and not equally accessible across different demographics and organizations. In recent years, the maturity of cloud technology has fostered the development of numerous business-to-consumer (B2C) self-paced training providers, making access to cybersecurity training and education much more widespread.

- **Continuous Professional and Experience Development (CPED):** Previously Continuous Professional Development (CPD), this process enables professionals to enhance their skills through self-reporting of accomplishments (e.g., certifications or seminars attended) and hands-on activities (e.g., delivering workshops, giving talks). As experimental content and cyber range solutions become more widely available, professionals can strengthen their profiles with ongoing practical experience, which is easier to validate than self-declaration methods.

3.2.2 Public-Private Partnerships

Public-private partnerships play a crucial role in addressing the cybersecurity workforce shortage. To maximize their impact, governments and businesses should take proactive steps to strengthen collaboration, accelerate workforce development, and ensure a steady pipeline of skilled cybersecurity professionals.

The following actions should be prioritized:

- **Research and Development (R&D) Capability-Building Programs:** Organizations can benefit from developing internal cybersecurity R&D capabilities, particularly when supported by knowledge-transfer programs with technology vendors and academic institutions. Employees gain specialized expertise through online courses, conferences, and university partnerships, while security-critical teams undergo intensive, long-term training to develop advanced skills. These programs help organizations enhance their in-house cybersecurity expertise while fostering innovation.

- **Workforce Development Activities:** Expanding workforce development initiatives allows governments and private sector leaders to better address the growing demand for cybersecurity professionals, particularly in underrepresented groups such as transitioning defense personnel and financially disadvantaged communities. These initiatives provide structured training, mentorship, and job placement opportunities, creating more accessible pathways into cybersecurity careers.

3.2.3 Artificial Intelligence

AI is emerging as a key tool for addressing the cybersecurity workforce shortage by enhancing training, education, and operational efficiency.

Figure 16 shows that 54% of organizations are considering using AI-powered assistants to help mitigate the skills gap. Meanwhile, nearly every major security vendor has incorporated AI into its products, highlighting its growing role in cybersecurity.

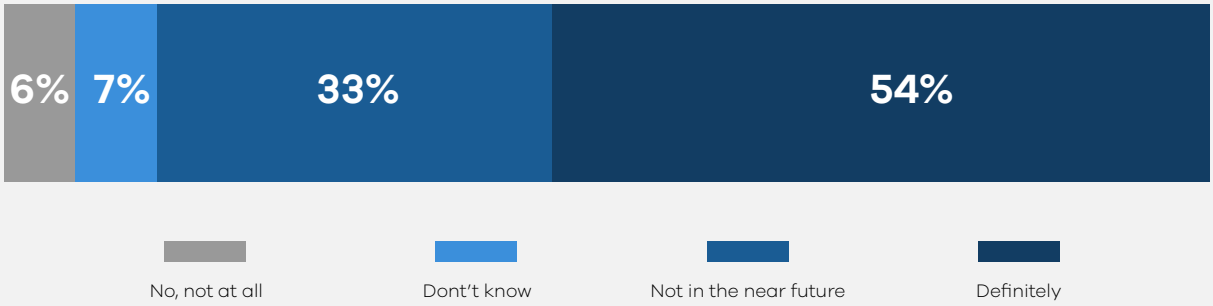


Figure 16: Organizations ready to acquire an AI agent to help mitigate the skills gap

While the long-term value of AI in cybersecurity training is still being evaluated, survey respondents expect its impact on performance and security training to be significant.

AI-driven advancements will improve workforce training and development in three key areas:

- **Adaptive Training and Education:** AI-powered systems can personalize content to individual strengths, weaknesses, and progress. Intelligent tutoring systems can provide human-like assistance in real time, adapting to the learner's progress and challenges to make training more efficient and engaging.

- **Realistic Simulation Environments:** AI enhances hands-on training through immersive and realistic cyberattack simulations. These virtual environments offer safe, risk-free scenarios for skills development, automating content generation and ensuring dynamic and adaptive learning.

- **Enhanced Assessment Capabilities:** AI shifts from traditional static knowledge tests toward practical, job-specific evaluations. Advanced systems that can utilize facial and behavioral analysis to detect anomalies, improving the integrity and predictive capabilities of assessments.

AI's most transformative impacts towards addressing the cybersecurity skills gap will be in content creation and simulation development, which is likely to happen in two phases:

- **Content Acceleration (3-year outlook):** This will involve developing AI-assisted content creation tools for content creators and instructional designers to streamline the creation of baseline content. Content creation is a bottleneck, particularly for experimental content and simulations. As AI advances, it could automate the generation of user emulation, and intricate simulations, significantly reducing manual effort.

- **Simulation Tailoring (3-5 Year outlook):** As AI advances to support human-led content creation, training simulations will become more dynamic, adapting in real time to user skill levels and goals. This will create a more personalized and effective learning experience.

As emerging technologies evolve and gain traction, it is evident that the next generation of cybersecurity professionals must develop skills across both Information and Communication Technology (ICT) and Operational Technology (OT) fields.

Workforce transformation is essential to ensuring resilience. Addressing the skills gap through technical training, experiential learning, and public-private partnerships will be key to developing a capable workforce. At the same time, cybersecurity roles are shifting, with AI and automation taking over routine tasks. As a result, leadership must adapt—focusing on guiding workforce development, allocating resources strategically, and ensuring accountability for cyber risk management.

Organizations that invest in continuous learning and structured workforce strategies will be better positioned to navigate the complexities of the future cybersecurity landscape.

4. Recommendations to Strengthen Future Cybersecurity Postures

As cyber threats become more sophisticated and attack surfaces expand, organizations must take a proactive and adaptive approach to cybersecurity. The rapid evolution of emerging technologies, coupled with increasing regulatory pressures and evolving threat actors, requires organizations to move beyond reactive defense strategies and toward a holistic, forward-looking cybersecurity posture.

4.1 MUST Framework

To stay ahead of evolving cyber threats, organizations must take a proactive approach. This report introduces MUST (Monitor, Understand, Strategize, and Transform) – a structured framework (Figure 17) designed to strengthen cybersecurity postures.

By adopting MUST, organizations can integrate emerging technologies effectively while also developing a skilled workforce, ensuring they are prepared to manage risks, enhance resilience, and drive long-term security success.

Figure 17: MUST framework

Effective implementation of the MUST framework to navigate cybersecurity challenges, close the skills gap, and build a robust, adaptive security strategy involves:

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 responsibilities for monitoring the development and adoption of emerging technologies (e.g., AI, IoT and quantum computing).
- **Partnerships and Alliances:** To stay ahead of technological advancements, establish strategic partnerships with vendors, research institutions, and peers. Examples include cybersecurity intelligence-sharing networks such as FS-ISAC (Financial Services Information Sharing and Analysis Center) for the financial sector, the Joint Cyber Defense Collaborative (JCDC) for cross-sector collaboration, and partnerships between national cybersecurity agencies and industry leaders, such as ENISA's work with private enterprises to strengthen cyber resilience in Europe. Leverage these partnerships to access cutting-edge cybersecurity solutions and insights.
- **Engage with Industry:** Actively participate in major industry events (e.g., forums, webinars, and conferences) such as RSA Conference, Black Hat and DEF CON, which bring together cybersecurity professionals, policymakers, and industry leaders, to remain informed about the latest trends, innovations, and best practices in cybersecurity.
- **Incorporate Frameworks:** Incorporate threat intelligence frameworks such as MITRE ATT&CK and NIST Cybersecurity Framework to track cyber risks associated with emerging technologies.
- **Monitor Regulatory Developments:** Monitor regulatory developments, including the EU NIS2 Directive, U.S. SEC Cybersecurity Disclosure Rules, ISO/IEC 27001 updates, and emerging technology policies such as the EU AI Act and NIST AI Risk Management Framework. Staying informed on evolving regulations ensures compliance, strengthens risk management, and enables organizations to align their cybersecurity strategies with the latest legal and industry standards for emerging technologies.

Understand: Gain a comprehensive insight into the ways emerging technologies influence the cybersecurity landscape and the benefits they can provide to your organization.

- **Impact Analysis:** Continuously reevaluate potential risks and benefits that emerging technologies may bring to your organization in terms of cybersecurity and the broader business context to identify promising applications. Stay up to date with emerging technology risk frameworks and global cybersecurity policy developments, such as NIST's Emerging Technology Research initiatives, which provide guidance on securing AI, quantum computing, and cryptographic advancements, as well as OECD's Digital Security Risk Recommendations, which outline policy frameworks for managing cybersecurity risks in the evolving digital landscape. Assessments should not only address present risks and opportunities but also incorporate science-based foresight scenarios to support strategic planning for future state evaluations.
- **Pilot Testing:** For promising technologies and applications, validate the potential benefits and challenges they may bring to your organization by conducting tests in a controlled environment. Collect data and insights from these tests to inform decision-making and refine the approach before broader implementation.

Strategize: Leverage emerging technologies in cybersecurity to enhance security measures, improve threat detection, and proactively protect from evolving threats.

- **Strategic Planning:** Based on findings from the Monitor and Understand phases, 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 researching, testing and implementing emerging technologies. Ensure investments align with the organization's risk appetite and strategic priorities.

Transform: Implement and adapt emerging technologies to enhance and strengthen the organization's cybersecurity posture.

- **Technology Integration:** Implement and scale technologies that have demonstrated the ability to fortify your organization's cybersecurity posture and deliver value.
- **Workforce:** Invest in training cybersecurity employees to equip them and prepare them in the new ways of cyber defense. Also, improve awareness among all employees regarding current and future cybersecurity opportunities and threats posed by emerging technologies.
- **Processes and Organization:** Align processes and organizational structures to support integrating emerging technologies.

4.2 Beyond the MUST Framework

Organizations that embrace a structured approach like the MUST framework can strengthen their security posture and stay ahead of emerging threats. However, cybersecurity resilience requires more than just technology and strategic planning; it is also shaped by awareness, regulatory enforcement, and collective action. A well-informed ecosystem, comprising organizations, policymakers, and law enforcement, plays a critical role in reducing risks and strengthening defenses across the cybersecurity landscape.

Recent research highlights this in the fight against ransomware, where global ransom payments fell to $813 million in 2024, down from $1.25 billion in 2023. This decline reflects stronger law enforcement efforts, effective regulatory oversight, and increased resistance to paying ransoms, driven by heightened awareness and improved preparedness.

While high-profile ransomware incidents still occur, this trend underscores the importance of proactive policy measures and cross-sector collaboration, reinforcing the notion that cybersecurity resilience is about more than just technology – it is also about governance, compliance, and shared responsibility for a secure future.

Conclusion

Technological advancements offer significant opportunities to enhance cybersecurity by improving threat detection and response. However, the rapid pace of innovation also introduces new vulnerabilities and increasingly sophisticated cyber threats. To effectively manage these risks, organizations must take a proactive approach – one that enables them to monitor, understand, strategize, and transform their cybersecurity practices. By staying ahead of emerging threats and integrating new solutions strategically, organizations can leverage technological advancements while minimizing associated risks.

At the same time, the cybersecurity workforce shortage and skills gap remain critical challenges. Without a skilled workforce, even the most advanced security technologies will fall short. Investing in continuous learning and development is essential to closing this gap and ensuring a more prepared cybersecurity workforce. Solutions include developing robust training programs, expanding access to security education, and fostering public-private partnerships. By addressing these workforce challenges, organizations can build the talent pipeline necessary to meet evolving cybersecurity demands.

Building a resilient cybersecurity posture requires more than just technology. It demands proactive strategies, global collaboration, and workforce development. By embracing these solutions, organizations and policymakers can navigate the evolving cybersecurity landscape with confidence, ensuring a secure and sustainable future.

Appendix – Methodology

This section details the methodology employed in our comprehensive analysis of the intersection of cybersecurity, technological acceleration, and workforce transformation. To ensure the robustness and depth of our findings, we utilized a blend of primary and secondary sources. The methodologies for each source are elaborated on below.

The main source of insights presented in the research was a detailed survey designed to capture expert insights on Technological Acceleration and Workforce Transformation. The survey comprised 43 questions and was distributed to a targeted group of cybersecurity and emerging technology experts across diverse sectors and roles. It was conducted from April to August 2024 and received 180 responses.

The Future of Cybersecurity Knowledge Community organized a 90-minute Community Meeting on April 30th, 2024, to supplement the survey data and gain deeper qualitative insights. The meeting brought together more than 25 representatives of the Knowledge Community and focused on knowledge exchange around emerging technologies.

Lastly, secondary data was sourced from reputable publications and reports. These sources were selected to ensure they aligned with the report objectives and provided relevant information. Citations for the secondary resources are interspersed throughout the report to support and enhance the primary research findings.

In conclusion, the mixed-method approach, combining robust primary data collection with supportive secondary research, provided a comprehensive and nuanced understanding of the future state of cybersecurity.

Appendix – Survey Demographics

The survey gathered data from diverse respondents across various sectors, roles, and regions. This section provides a detailed demographic analysis based on the data collected from the participants. Category 'other' groups all records that represent less than 5% of the total survey respondents.

Sector Representation

As shown in Figure 18, most survey participants were from the private sector, constituting 82% of the respondents. This was followed by public sector or governmental entities at 13% and academia or NGOs at 4%. This distribution highlights a significant leaning towards private sector involvement in the survey.

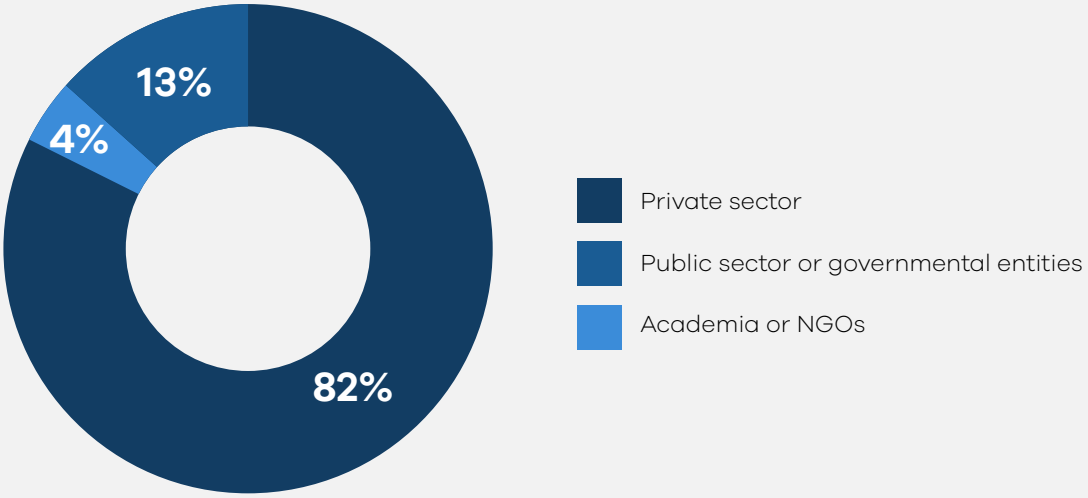


Figure 18: Sector representation of the survey respondents

Organizational Roles

Figure 19 shows that survey participants occupied various organizational roles. Executives represented 25% of the respondents, professional staff accounted for 36%, and managerial/ non-executive roles comprised 39%. This distribution suggests a balanced representation of different hierarchical levels within organizations.

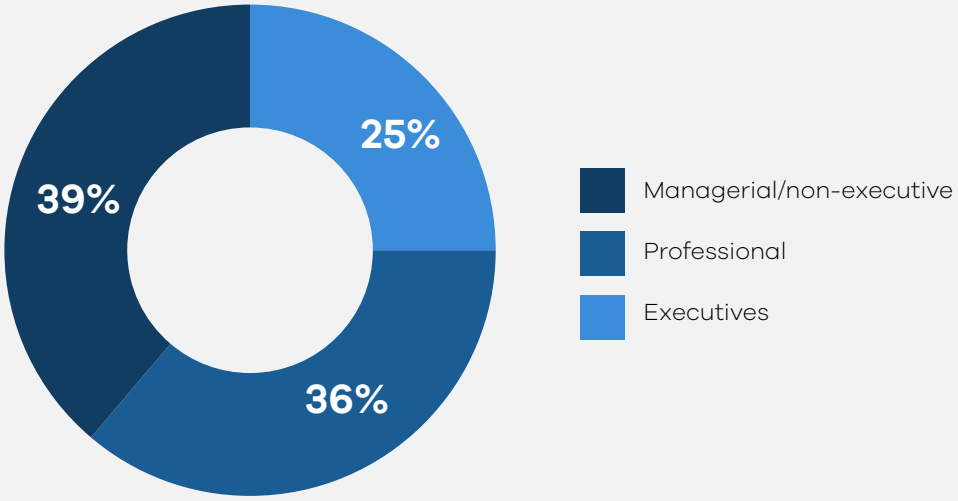


Figure 19: Organizational roles of the survey respondents

Headquarters Location

The geographical distribution of the respondents was varied (Figure 20), with the largest group from North America (29%) and Europe and Central Asia (28%). Other regions included East Asia and Pacific (6%), South Asia (2%), Middle East and North Africa (20%), Latin America and Caribbean (12%), and Sub-Saharan Africa (3%). This showcases global participation in the survey.

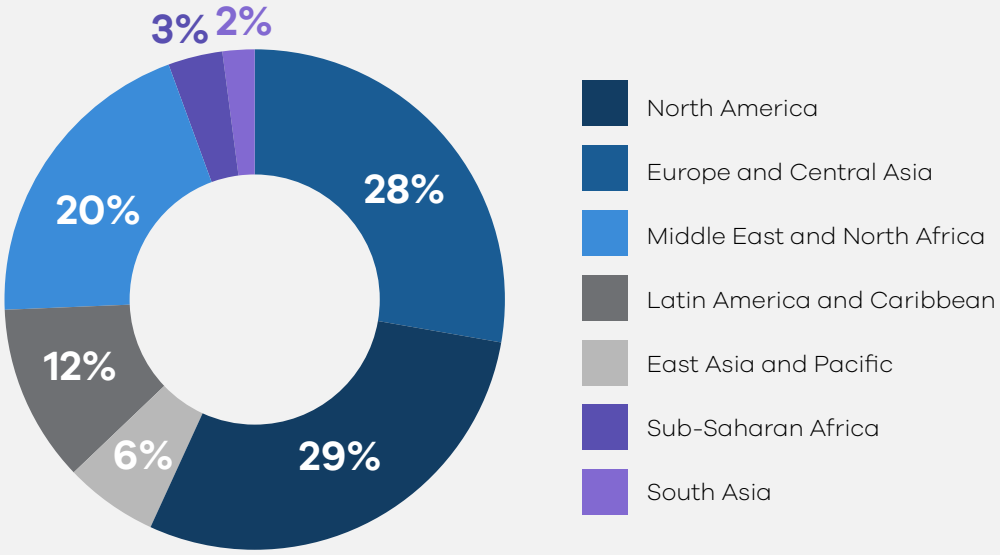


Figure 20: Headquarters location of the survey respondents

Job Functions

Participants' job functions were categorized into several areas (Figure 21): C-suite (e.g., CEO, President) roles made up 11%, Information Security roles accounted for 39%, IT/Technology roles were 26%, R&D roles constituted 5%, and other roles were 19%. The predominance of information security and IT/ Technology roles underscores the survey's relevance to these fields.

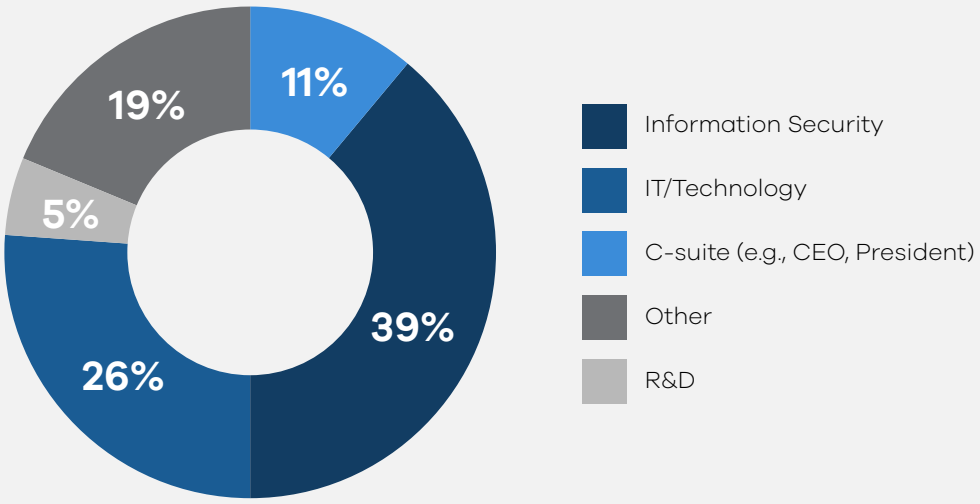


Figure 21: Job functions of the survey respondents

Years of Experience

The survey also captured the respondents' professional experience (Figure 22). Those with less than five years of experience were 35%, 5-10 years at 30%, 11-15 years at 17%, 16-20 years at 9%, and those with more than 20 years at 8%.This distribution reflects a broad range of professional experience among the respondents, with a significant portion having substantial industry experience.

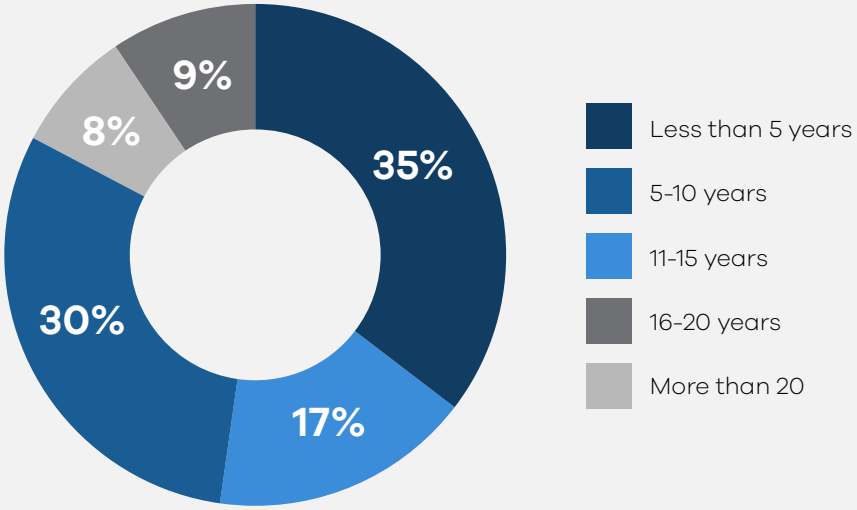


Figure 22: Years of experience of the survey respondents

Endnotes

1. Global Cybersecurity Forum (September 2024). Navigating GenAI Threats and Opportunities in Cybersecurity.
2. Global Cybersecurity Forum and Boston Consulting Group (October 2024). 2024 Cybersecurity Workforce Report: Bridging the Workforce Shortage and Skills Gap
3. Innov-acts (July 2023). The Impact of Generative AI on Cybersecurity: Opportunity or Challenge?
4. Electronic Frontiner Foundation (June 2022). Keeping your smart home secure
5. Appleyard Lees (January 2024). Certainty in the trajectory of patents for quantum computing
6. BCG (September 2024). It's time to implement new tools to counter quantum hacking
7. ISC2 (September 2024). Cybersecurity Workforce Study


GLOBAL
CYBERSECURITY
FORUM
Site