



2024 CYBERSECURITY WORKFORCE REPORT:

Bridging the Workforce
Shortage and Skills Gap



The Global Cybersecurity Forum (GCF) is a global, non-profit organization that seeks to strengthen global cyber resilience by advancing international multistakeholder collaboration, purposeful dialogue, and impactful initiatives. It serves as a platform where the world's cybersecurity stakeholders exchange knowledge and collaborate in tackling critical issues around Cyberspace. GCF aims to catalyze socioeconomic change, push the knowledge boundaries on critical cybersecurity topics, and build the foundations for global cooperation on key challenges and opportunities in Cyberspace. By uniting decision makers and thought leaders from around the world, GCF aligns with international efforts to build a safe and resilient Cyberspace that is an enabler of prosperity for all nations and communities.

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders—empowering organizations to grow, build sustainable competitive advantage, and drive positive societal impact.

Our diverse, global teams bring deep industry and functional expertise and a range of perspectives that question the status quo and spark change. BCG delivers solutions through leading-edge management consulting, technology and design, and corporate and digital ventures. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, fueled by the goal of helping our clients thrive and enabling them to make the world a better place.



Executive Summary

The 2024 Cybersecurity Workforce Report reveals a critical shortfall of professionals, creating substantial challenges for organizations worldwide. Despite an annual investment of nearly \$200 billion annually in cybersecurity products and services, businesses are struggling to keep pace with escalating cyber threats, with only 72% of cybersecurity roles being filled.

The global cybersecurity workforce currently stands at 7.1 million professionals, with significant regional disparities. Asia-Pacific, led by India and China, has the largest workforce in absolute terms, followed by the Americas and then Europe. The U.S. leads in cybersecurity maturity, housing 70% of the world's cybersecurity vendors, while China and India are rapidly emerging as cybersecurity hubs. However, Africa is severely underrepresented, with fewer than 300,000 cybersecurity professionals. These differences across geographies reflect common global development indicators and highlight varying levels of cybersecurity maturity.

The report identifies a global shortfall of 2.8 million cybersecurity professionals. Alarmingly, less than four qualified professionals exist to fill every five cybersecurity jobs. Asia-Pacific is facing the most acute deficit, accounting for 60% of the global shortage. This shortage is driven by years of underinvesting coupled with rising importance of cybersecurity. The shortage is regional as well as industry-specific, with sectors like Financial Services, Technology, and Materials and Industrials collectively accounting for 64% of the workforce shortage. About 64% of respondents to our survey identified the primary challenge in filling cybersecurity positions being a lack of qualified candidates.

Emerging technologies, especially generative AI (GenAI), are transforming the cybersecurity landscape at an unprecedented pace. While these technologies offer significant benefits, they also expand the attack surface and create new vulnerabilities. According to our research, 70% of organizations have already integrated AI into their cybersecurity frameworks, leveraging it for anomaly detection, predictive analytics,

and network traffic monitoring. However, these advancements pose risks too, with 58% of cybersecurity leaders expressing concern over new adversarial techniques and AI-enabled cyberattacks.

In response to these challenges, the report emphasizes the need to shape the cyber workforce of tomorrow. Rapidly evolving technologies require continuous upskilling of cybersecurity professionals, with 60% of organizations identifying ongoing training as essential to maintaining an effective cybersecurity team. Building a future-ready workforce involves fostering a culture of continuous learning, offering both internal and external training programs, and aligning skillsets with the latest threat trends. Organizations are increasingly implementing proactive skill mapping and gap analysis to address skill gaps before they become critical. By investing in education and creating clear career pathways, organizations can ensure their cybersecurity teams are prepared to navigate the complexities of an ever-changing cybersecurity environment.

There is a pressing need to attract new talent by promoting diversity and inclusion, with a particular emphasis on empowering underrepresented groups, especially women. Despite comprising 36% of broader tech roles, women represent only 24% of the cybersecurity workforce. Increasing participation from women in cybersecurity would do more than fill the empty chairs, it is a sure-shot win-win by broadening and strengthening cybersecurity capabilities, and improving business performance.

Addressing the cybersecurity workforce shortage requires targeted recruitment, continuous training, and an inclusive environment that fosters growth and retention, attracting significantly more talent to the field, intensifying education and training initiatives, recruiting the right professionals, and ensuring stronger retention of cybersecurity experts. A coordinated effort in these areas is essential to building a resilient cybersecurity workforce for the future.

Contents

01. Decoding the Global Cybersecurity Workforce Shortage	05
02. Diversity Bridge: Empowering Women to Work in Cybersecurity is a Sure Shot Win-Win	14
03. A Cyberworld in the Midst of Rapid Technological Transition	19
04. Shaping the Cyber Workforce of Tomorrow	22
05. Call to Action: A Roadmap to Success	25
06. Building the Next Generation of Cyber Defenders	29
07. Methodology	31



01.

DECODING THE GLOBAL CYBERSECURITY WORKFORCE SHORTAGE

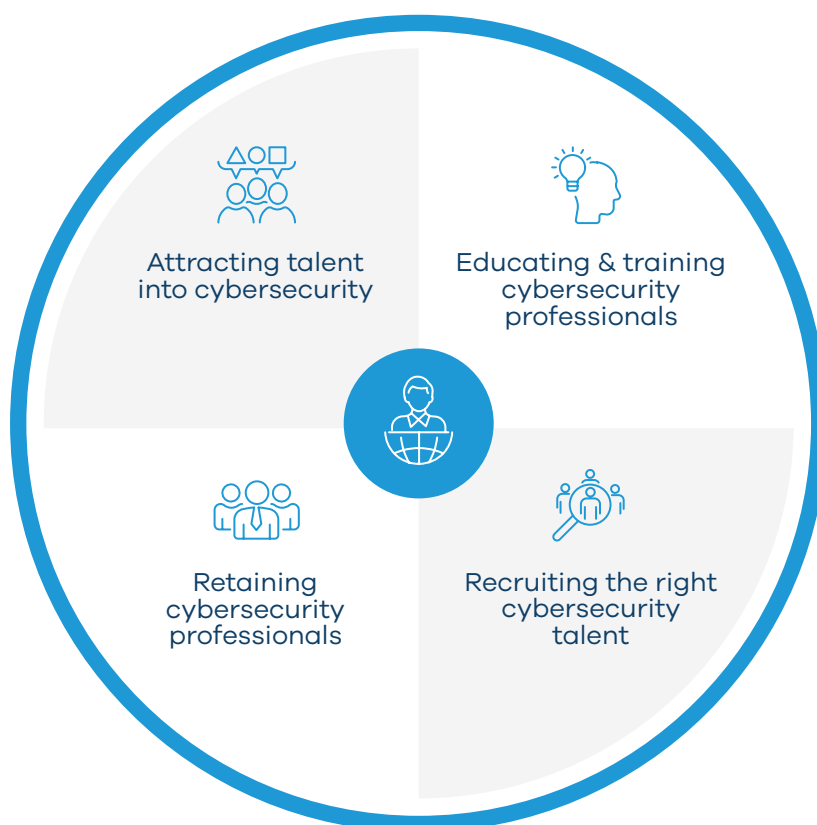


As the boundaries between the cyber and physical worlds continue to blur, cybersecurity leaders are expressing alarm; roughly 85% highlight the rise in the frequency of cyberattacks as a rapidly growing cause for concern.¹ The global cost of cybercrime is estimated to have risen from \$445 billion in 2015 to over \$2.2 trillion today,² underscoring the urgent need for heightened attention to this critical challenge.

So far, organizations worldwide have responded by investing nearly \$200 billion annually in cybersecurity products and services.³ But this investment alone is not enough. There is a critical need for more skilled professionals, yet a shortage of cybersecurity professionals is leaving many organizations and countries increasingly vulnerable.

The cybersecurity workforce deficit is often discussed in terms such as “skills shortages” or “workforce gaps,” which are used interchangeably despite their distinct nuances. This inaccuracy leads to confusion and misunderstanding regarding the specific type of scarcity that the industry faces and the targeted actions needed to solve the issues. “Workforce shortage” highlights the overall deficit of professionals qualified for any cyber positions, while “skills gap” refers to the disconnect between the skills that organizations need and those currently possessed by the workforce. These interrelated challenges are central to our analysis of the cybersecurity industry’s workforce challenges.

Exhibit 1 - The Cybersecurity Talent Framework



Source: World Economic Forum, 2024

1. Navigating the New Cybersecurity Environment | BCG

2. BCG Analysis

3. Gartner

The global cybersecurity workforce comprises 7.1 million professionals. The Asia Pacific region, driven by China and India, has the largest cybersecurity workforce with roughly 2.9 million professionals (Exhibit 2).

The Americas, with 2.4 million professionals, demonstrates a strong commitment

to cybersecurity. Europe follows with 1.4 million. In contrast, Africa lags behind other regions with just 0.3 million professionals. These differences across geographies reflect common global development indicators and highlight varying levels of cybersecurity maturity.

Exhibit 2 - Region-wise view of current cybersecurity workforce



Source: Survey results

The United States boasts the largest cybersecurity workforce globally, a testament to its pioneering cyber maturity and its position as the headquarters for approximately 70% of the world's leading cybersecurity vendors.⁴ China is rapidly emerging as a formidable near-peer in terms of cyber headcount, driven by its rapid digitization efforts and substantial investments in cutting-edge technologies.

The rise of Global Capability Centers (GCCs)/ Shared Service Centers (SSCs) has further reshaped the global cybersecurity workforce. These centers, which are instrumental

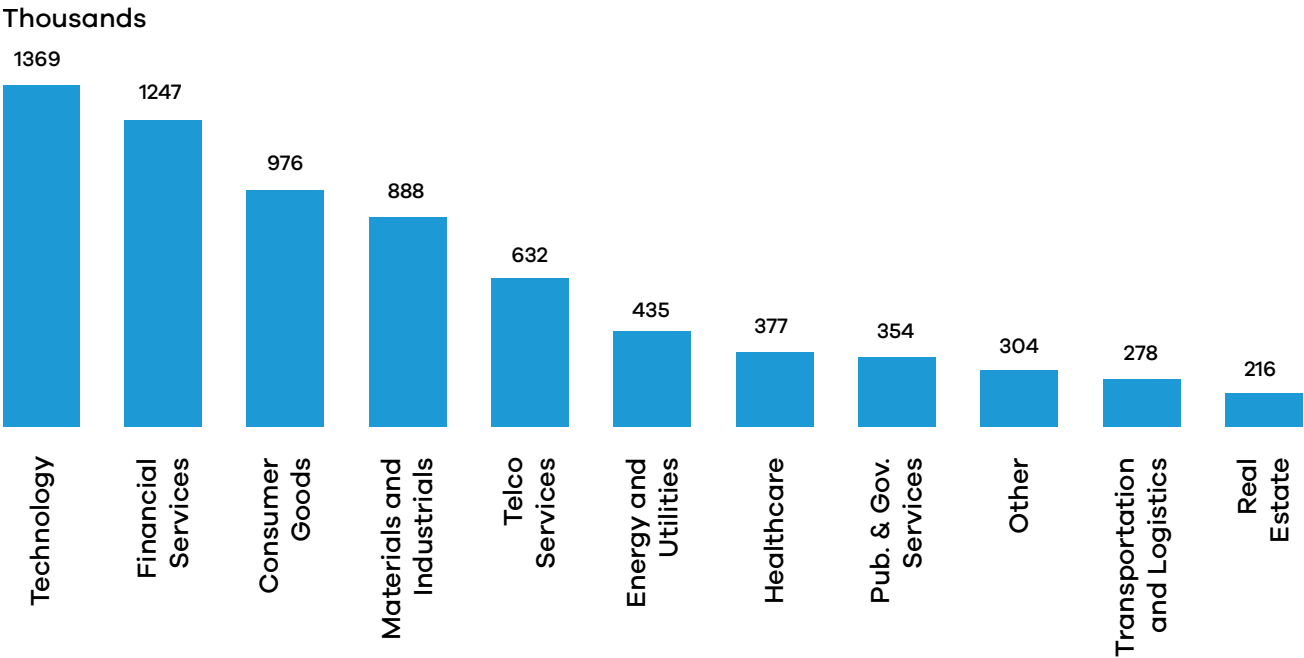
in setting strategic direction, enhancing governance, and embedding a "security and safety by design" ethos across industries, have catalyzed the growth of sizable cybersecurity workforces in countries like India, Mexico, and Brazil. Notably, India is emerging as a pivotal force in the global cybersecurity arena with an increase of GCC setups and outsourcing.⁵

4. Gartner
5. NASSCOM

The distribution of the cybersecurity workforce varies across industries. The top two industries having largest cybersecurity workforces are Technology and Financial Services companies. Tech leads with approximately 19% of the

global cybersecurity workforce, mainly due to its dual role as both a provider and consumer of cybersecurity products and services, followed by Financial Services with 18% (Exhibit 3).

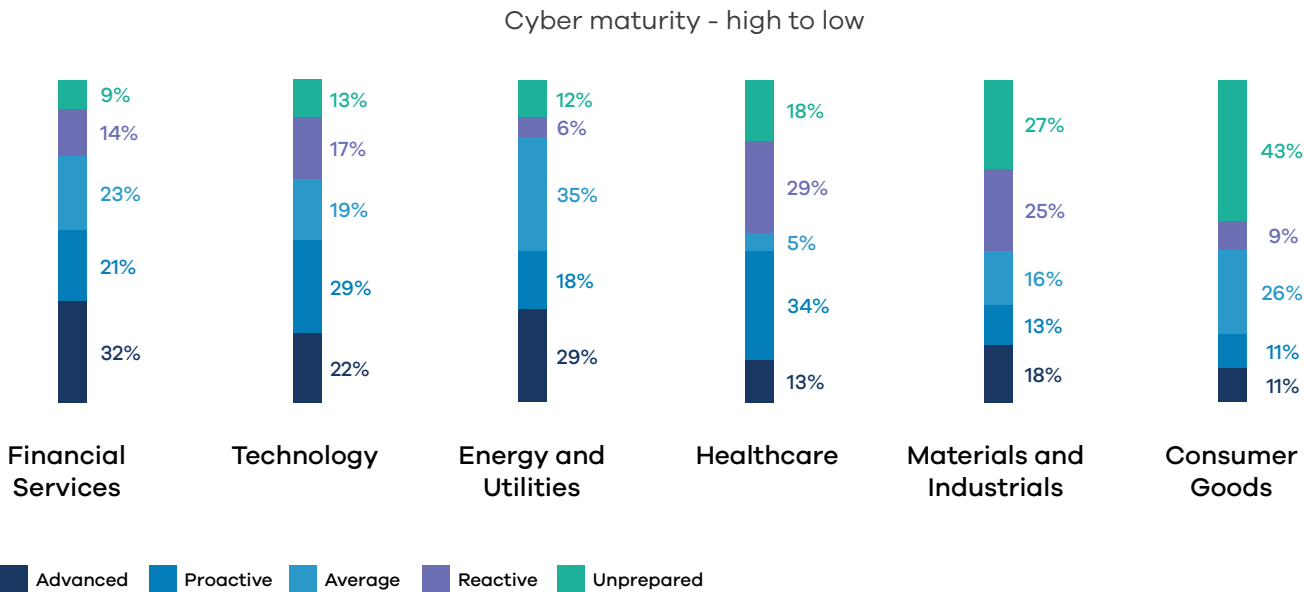
Exhibit 3 - Distribution of cybersecurity workforce per industry



These figures mirror both industries’ scores in BCG’s 2024 CISOs survey and reflect their disproportionate spending on cybersecurity (Exhibit 4).

Interestingly, Consumer Goods and Materials & Industrials collectively account for 26% of the cybersecurity workforce, driven primarily by the sheer sizes of both industries.

Exhibit 4 - Self-reported cyber maturity across industries

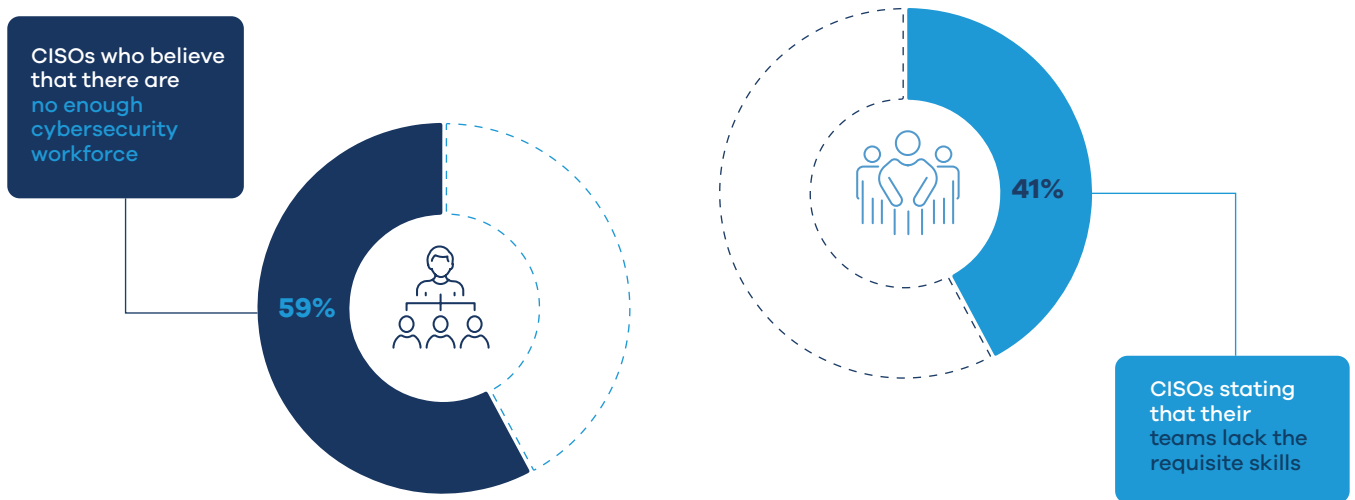


Please note: Media, Professional Services, Education not displayed
Source: BCG & GLG CISO Survey, 2024

Global Cybersecurity Workforce Shortage

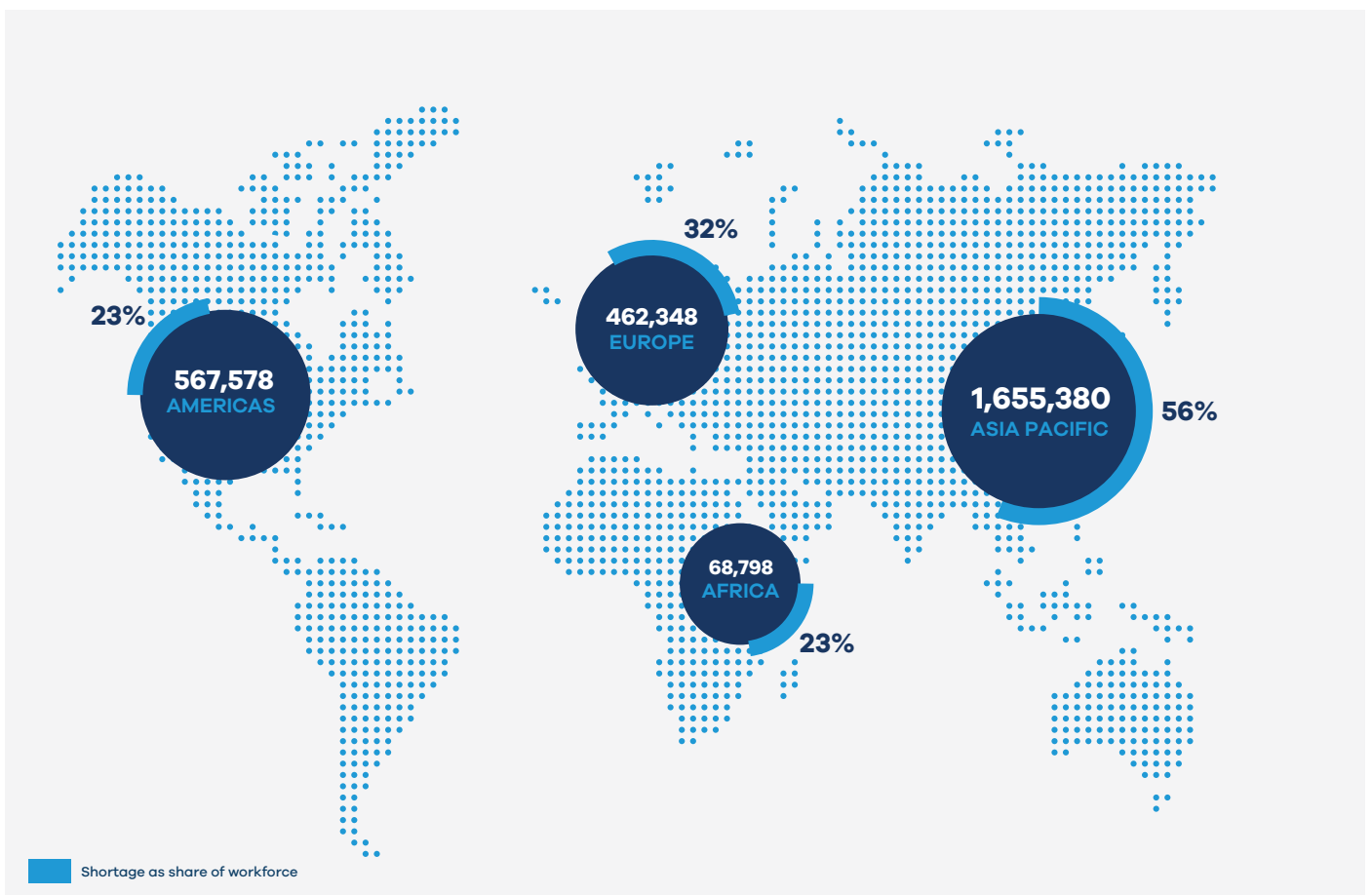
Our analysis reveals a critical global cybersecurity workforce shortage of 2.8 million professionals. Alarming, less than four qualified professionals exist to fill every

five cybersecurity jobs, and 59% of CISOs say workforce shortage is a “top barrier for achieving their security posture.”⁶ Projections suggest that the shortage is to become the key factor behind more than 50% of significant cybersecurity incidents worldwide.⁷



Source: BCG 2024 CISO survey

Exhibit 5 - Regional view of current cybersecurity workforce shortage



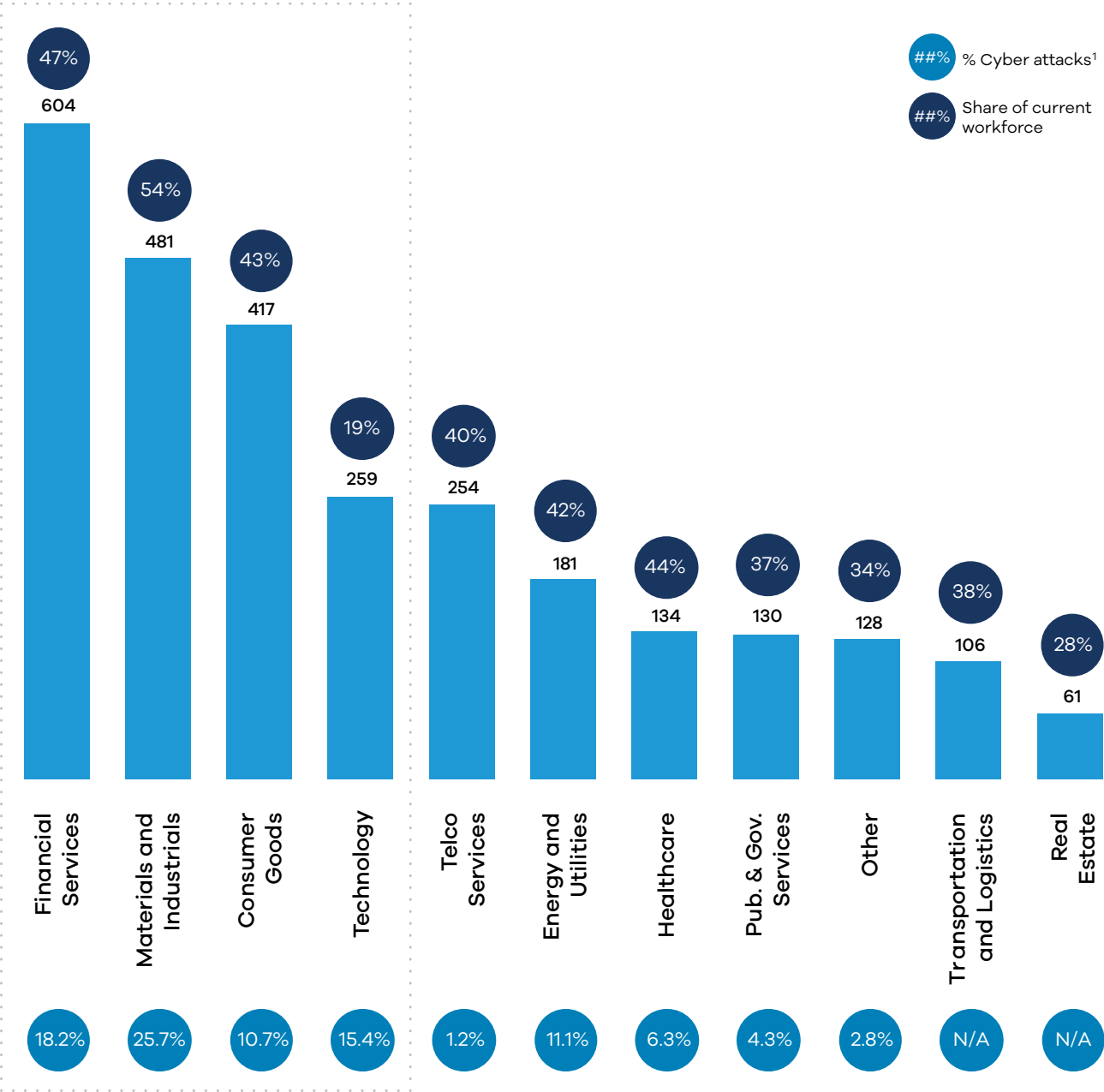
Source: Survey results

6. BCG 2024 CISO survey
7. Gartner

The Asia-Pacific region is particularly affected, with a shortage equivalent to 56% of its current workforce. This acute shortage is primarily due to the region’s relatively low cybersecurity maturity and emerging recognition of the field’s importance. In Europe and the Americas, the shortage is smaller relative to their respective workforces but remains considerable in absolute terms. In Africa, the shortage is smaller in absolute numbers but still represents 23% of the cybersecurity workforce.

Approximately 64% (Exhibit 6) of the cybersecurity workforce shortage is disproportionately concentrated in four industries: Financial Services, Materials and Industrials, Consumer Goods, and Tech. This is unsurprising given that they are the target of approximately 70% of all global cyber attacks, and that the cost per breach for each of these industries also tends to be the highest.⁸

Exhibit 6 – Shortage of cybersecurity workforce per industry



1. Adapted from IBM
Source: IBM, Survey results

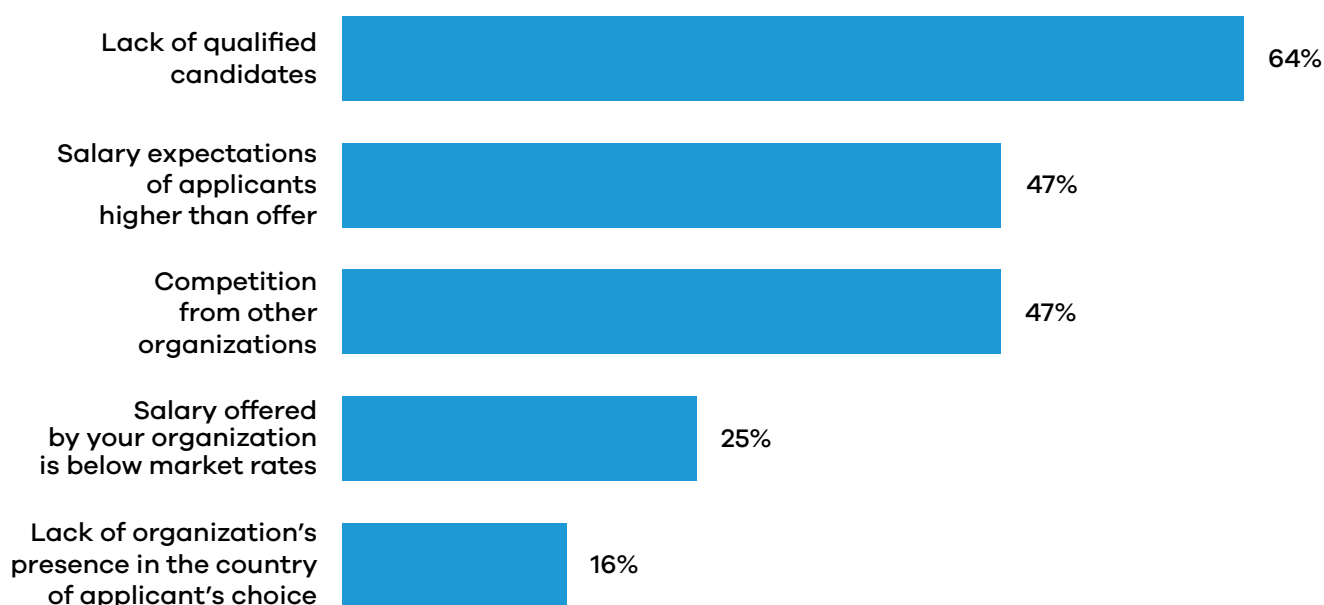
8. IBM

Comparison of the shortage with the current workforce reveals that the shortage is most acute in the Materials and Industrials sector, accounting for 54% of the current workforce, followed by Financial Services at 47%, and Healthcare at 44%. Unsurprisingly, the Tech industry has the least acute shortage, accounting to 19% of the current workforce, indicating that it is the top choice for cybersecurity talent.

Our analysis shows that among the myriad reasons behind the continuing cybersecurity workforce shortage, organizations struggle to hire due to a mismatch between the supply and demand of professionals in the field.

- **Short supply:** About 64% of survey respondents identified the primary challenge in filling cybersecurity positions being a lack of qualified candidates.
- **High demand:** Intense competition from other organizations, including those in other regions, was highlighted as a major challenge by 47% of respondents.

Exhibit 7 – Biggest challenges in filling cybersecurity positions



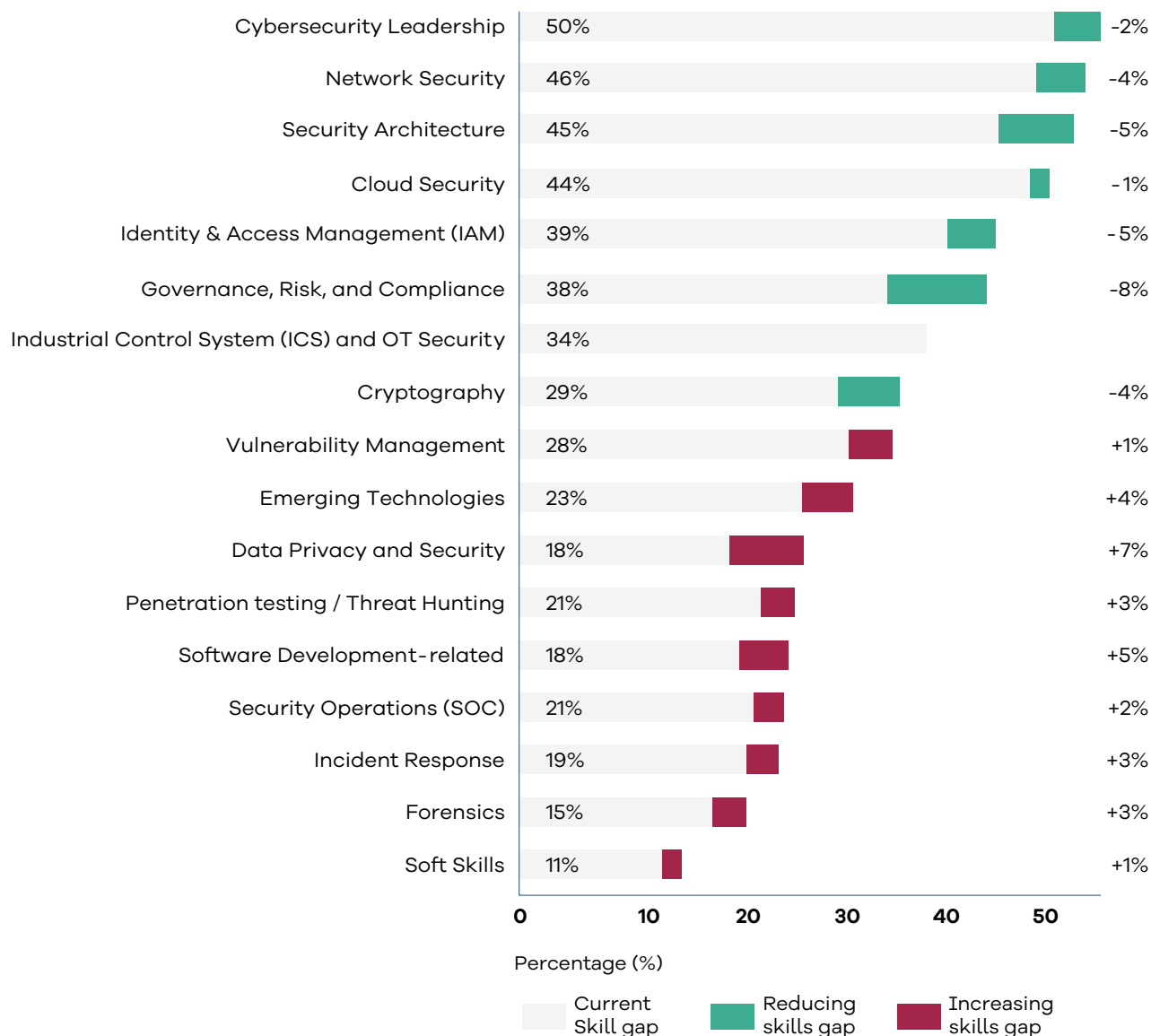
Source: Survey results

As cybersecurity continues to grow in importance, the shortage of a skilled workforce presents a critical challenge, with 43% of CISOs stating that their teams lack the requisite skills.⁹ Addressing this issue goes beyond simply increasing the number of professionals; it requires continuously updating skills to keep pace with the rapid evolution of cyber threats. Although this may seem straightforward in theory, the reality is far more complex in practice.

According to **the BCG Skills Disruption Index**, cybersecurity skills are evolving at one of the fastest rates across industries. As technological advancements accelerate, so too does the demand for new, specialized skills. This widening gap between the skills employees possess and those required to protect against emerging threats is expected to grow significantly. Exhibit 8 illustrates the projected evolution of this skills gap over the next five years.

9. BCG 2024 CISO survey

Exhibit 8 – Expected skill gap change in 5 years



Source: Survey results

The most significant skill gaps in areas such as cybersecurity leadership, network security, security architecture, and cloud security are projected to persist for at least the next five years. These areas demand a rare combination of technical expertise, business acumen, and deep security knowledge—essential to bridging the skills gap both directly and effectively.

- **Cybersecurity leadership** is the most pressing concern, with 50% of organizations identifying it as their top challenge now and in five years. The convergence

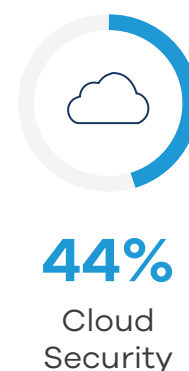
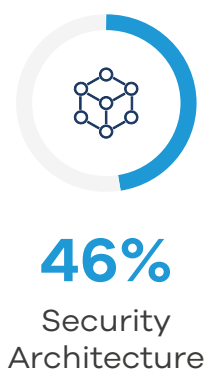
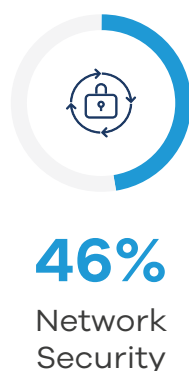
of cybersecurity and business acumen is essential yet difficult to find among the existing cadre of professionals.

- **Network security and security architecture** skills are among the top five hardest to source and will remain so in the future. The demand for these skills is heightened by the need for candidates with prior IT experience, which makes this gap particularly challenging to address.
- **Cloud security** skills are also in high demand, driven by the widespread shift

to cloud-based services. Cloud spend will account for 58% of IT Spending in 2027, up from 43% in 2022.¹⁰ However, 44% of organizations report they are struggling to find the necessary expertise—a challenge that is expected to continue as IT budgets increasingly prioritize cloud solutions.

- **Data Privacy and Security** expertise requirements are also expected to rise in demand, spurred by expanding global data privacy regulations. This growing need will further strain an already tight labor market.

Most challenging skill to be found



It is worth noting that 73% of organizations have not reported facing significant struggles in finding the skills related to emerging technologies. This suggests that most organizations focus on securing basic skills—a prudent approach when fundamental security measures are not yet fully in place. Hiring experts to address advanced threats and secure emerging technologies is seen as a luxury rather than a necessity for many organizations.

Additionally, while the cybersecurity skills gap is a pervasive challenge across industries, sector specific nuances exist. The increasing convergence of information and operational technology in industries such as Materials and Industrials is leading to significant issues in filling roles across industrial control system (ICS) and operational technology (OT) security.



10. Gartner



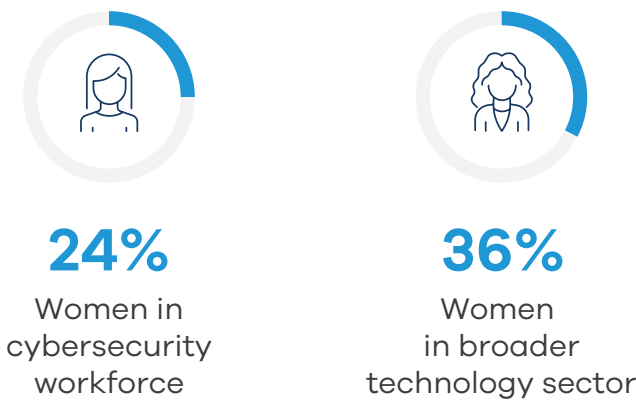
02.

**DIVERSITY BRIDGE:
EMPOWERING WOMEN
TO WORK IN CYBERSECURITY
IS A SURE SHOT WIN-WIN**

Leveraging underrepresented talent pools offers an opportune solution towards expanding the numbers and capabilities of the global cybersecurity workforce. The urgency of pursuing the inclusion of women in the field has never been greater, and attracting the demographic to the field is imperative for enhancing cyber resilience. According to

our research, organizations with less gender diversity tend to have more unfilled positions than similar organizations. This suggests they may be less attractive to candidates, highlighting the need for an inclusive environment to effectively address workforce shortage.

Empowering Women to work in Cybersecurity requires more efforts



Women comprise only 24% of the current global cybersecurity workforce, compared to 36% in the broader technology industry,¹¹ highlighting a severe gender gap in cybersecurity.

This disparity is not uniform across regions, with participation rates ranging from 25.4% in more digitally mature regions to 13.5% in those less mature (Exhibit 9).

Exhibit 9 – Share of women in cybersecurity workforce per region

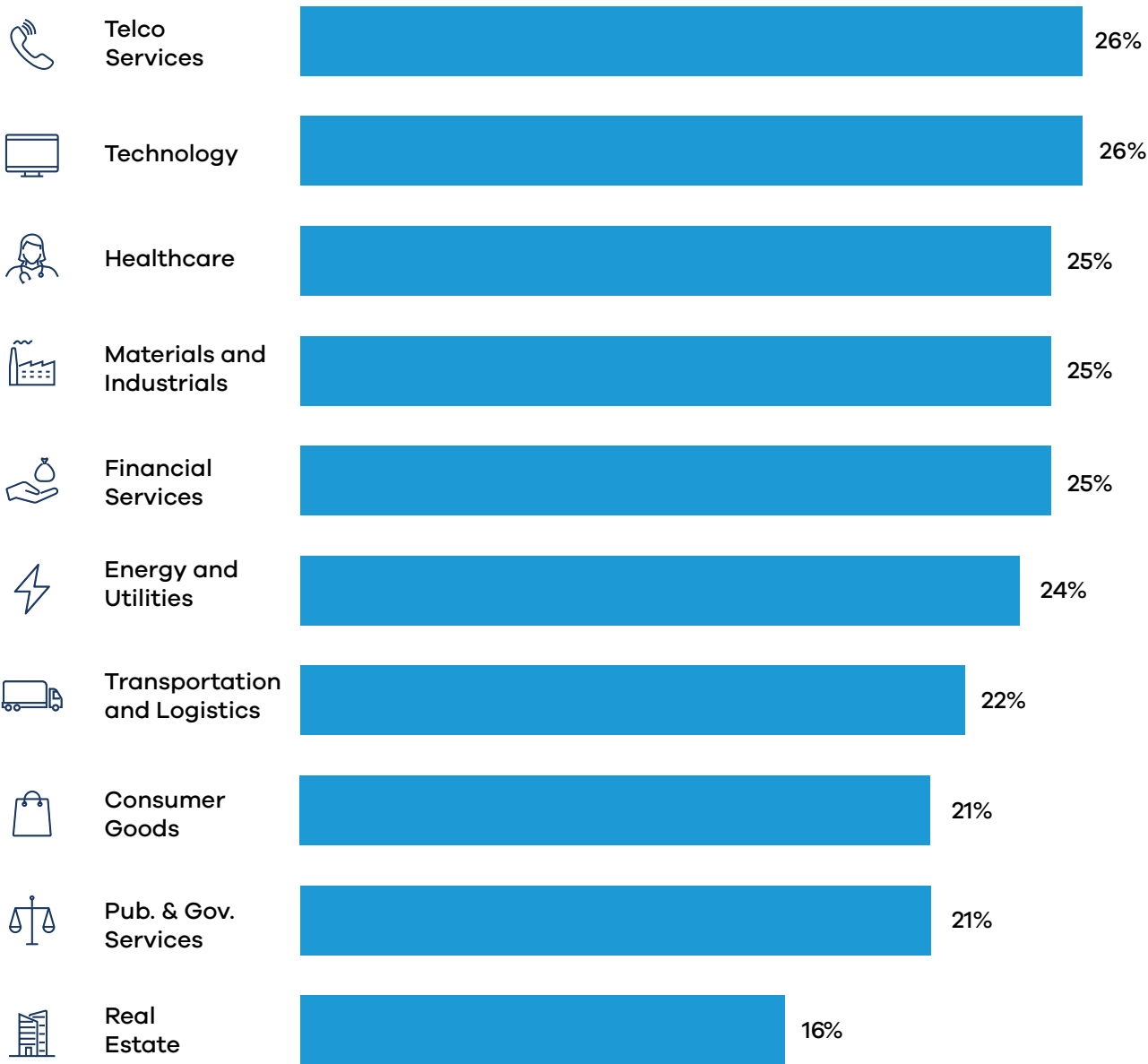


Similarly, more mature cybersecurity industries, such as Telecommunications, Technology, and Financial Services, have higher participation rates than those lower. Additionally, according

to a report by Forrester, only 16% of all CISOs are women¹². These figures underline the pressing need for more focused efforts to enhance gender diversity in cybersecurity roles globally.

11. World Economic Forum, Forrester

Exhibit 10 – Share of women in cybersecurity workforce per industry

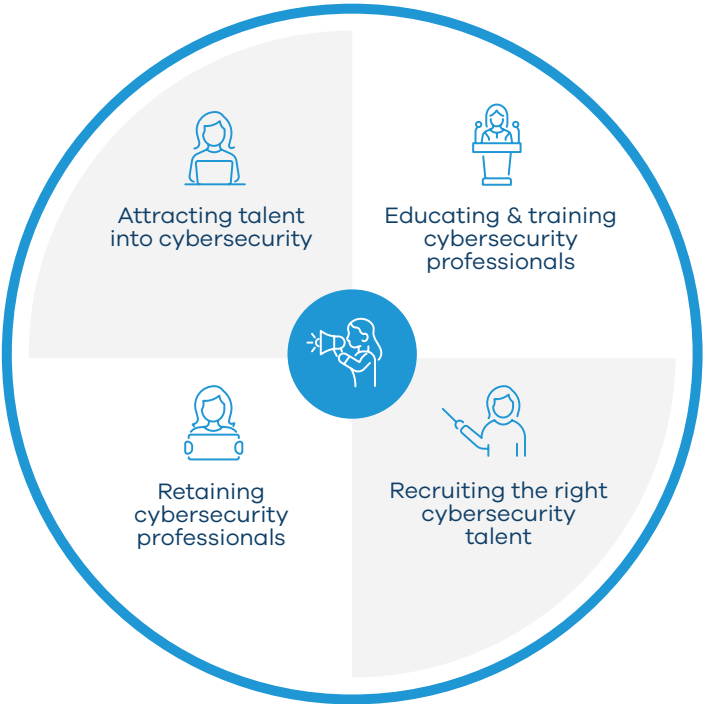


Source: Survey results

Attracting women to cybersecurity would do more than fill the empty chairs. It helps with:

- **Broadening and strengthening cybersecurity capabilities:** New talent pools can bring diverse perspectives and unique approaches to problem solving and innovation.
- **Improving business performance:** Research shows that diversity pays dividends; companies with a gender-diverse employee base tend to have financial returns that top national industry averages.¹²
- **Strengthening and diversifying national economies:** Encouraging women to pursue careers in cybersecurity can help strengthen a well-paying, highly productive, and future-proof industry.

12. Closing the Gender Gap in Investing | BCG



1 Attracting talent into cybersecurity

- Few visible and accessible women to serve as role models
- A lack of women to serve as mentors and sponsors
- Difficulty for women entrepreneurs to access resources

2 Educating & training cybersecurity professionals

- Low enrollment in STEM disciplines
- Feeder industries dominated by men
- Low awareness of cybersecurity
- Few role models
- Negative perceptions of cybersecurity

3 Retaining cybersecurity professionals

- Dropout and difficulty taking time off and returning to work
- Workplace discrimination and bias
- Long working hours
- A lack of professional development
- Impostor syndrome, elitism, and a low sense of belonging

4 Recruiting the right cybersecurity talent

- Unequal access to the job market and entrepreneurship
- Lack of access for nontechnical, non-STEM entrants
- A perception of the industry as masculine
- Discrimination against recruiting younger women of child-bearing age

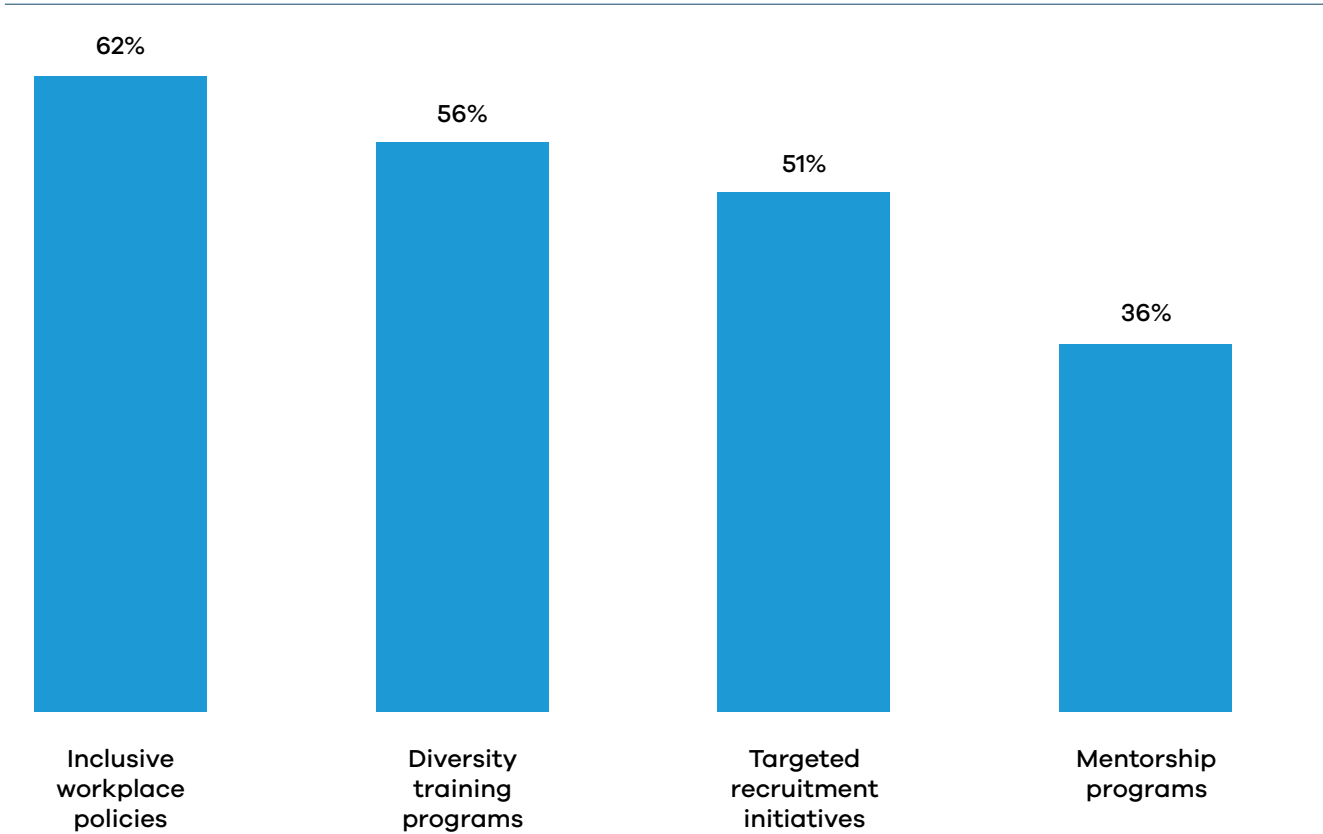
Having diversity, equity, and inclusion (DEI) initiatives benefits organizations beyond just increasing the talent pool. Our analysis shows that organizations implementing more DEI initiatives have higher employee satisfaction. Hence, it is not a surprise that most organizations have introduced several DEI initiatives such as:

- **Pipeline:** Our survey shows that 56% of organizations are running diversity training programs, which are key for creating an inclusive culture and changing the perception of cybersecurity as being a male-only industry.
- **Recruitment:** Approximately 51% of organizations have adopted targeted recruitment initiatives to attract more women into cybersecurity roles. These initiatives are crucial as they directly address the entry-point barriers by actively seeking out women candidates and encouraging them to apply for roles in what has traditionally been a field underrepresented by women.

- **Retention:** Roughly 62% of organizations have implemented inclusive workplace policies, which play a significant role in retaining women once they enter the cybersecurity workforce. These policies often include flexible working arrangements, parental leave, and support for work-life balance, all of which are essential in creating an environment where women are empowered to thrive.
- **Advancement:** Finally, 36% of organizations have established mentorship programs, which are particularly impactful in supporting the career development of women in cybersecurity.

The results from implementing this approach have so far been extremely encouraging. More women are entering cybersecurity than ever before, doubling their participation rate in just three years between 2017 and 2020.¹³ Continued efforts to empower women to participate in cybersecurity will bolster gender equality and strengthen cyber resilience.

Exhibit 12 – Initiatives implemented by organizations to increase diversity and inclusion in cybersecurity roles



Source: Survey results

13. ISC2

03.

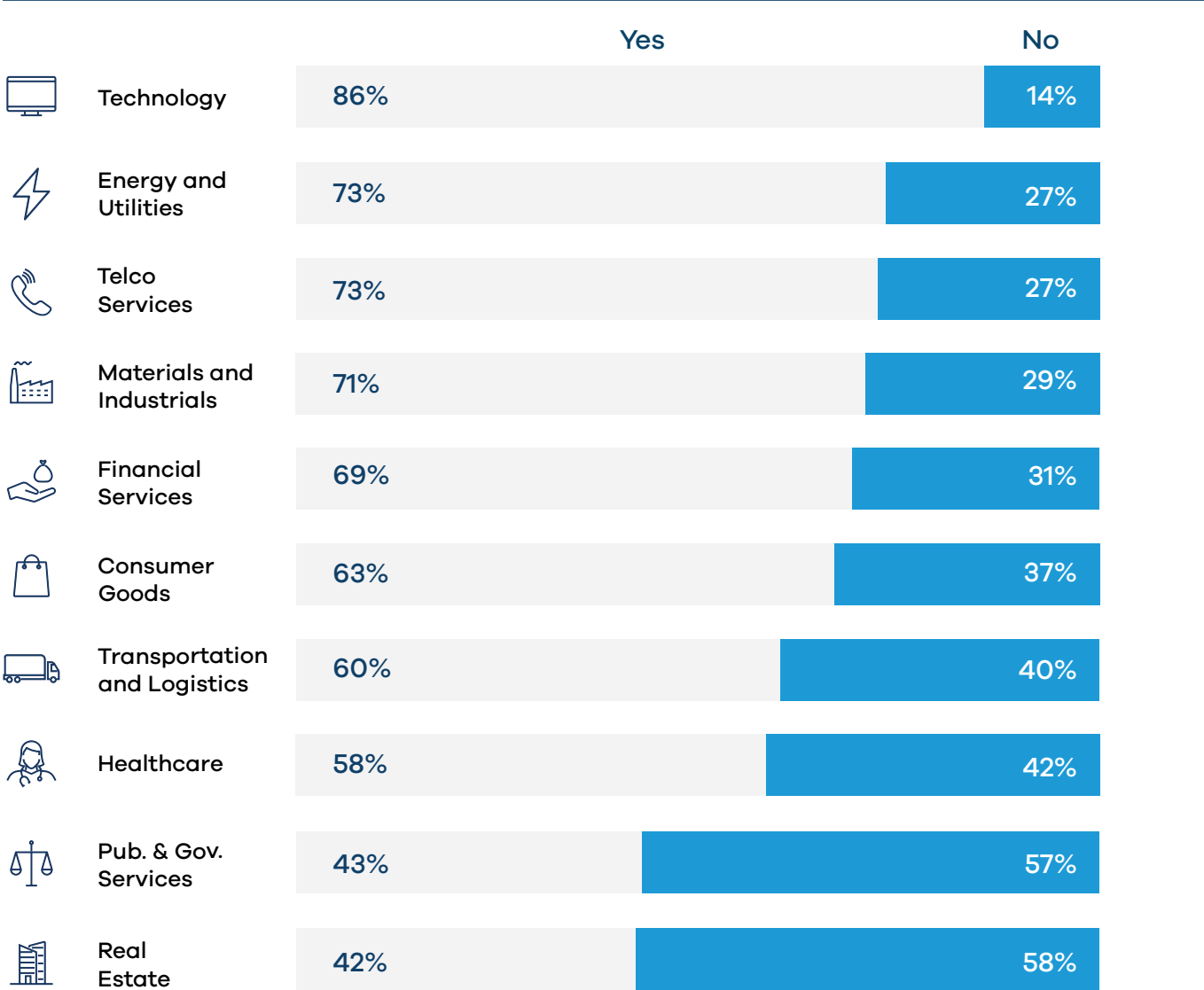
A CYBERWORLD IN THE MIDST OF RAPID TECHNOLOGICAL TRANSITION



Cybersecurity’s complexities have always grown in tandem with the rapid pace of technological advancement. However, the field is entering a new paradigm where emergent technologies, such as GenAI, offer tremendous benefits but pose equally serious risks.

AI, and especially GenAI, not only increases a company’s exposure to technology risks but also expands the potential attack surfaces of an organization, escalating the severity of threats both for businesses and the broader public.

Exhibit 13 – Share of organizations that leverage GenAI for cybersecurity operations per industry



Source: Survey results

Our survey shows that 70% of organizations have already integrated AI or GenAI into their cybersecurity operations, leveraging its capabilities mostly for anomaly detection, predictive analytics, and network traffic analysis. However, the penetration of GenAI in cybersecurity operations varies by industry. Mature industries tend to embrace GenAI more

readily than those with lower cybersecurity maturity levels. Additionally, GenAI can enhance productivity by automating routine cybersecurity tasks such as log analysis, vulnerability scanning, and incident reporting.

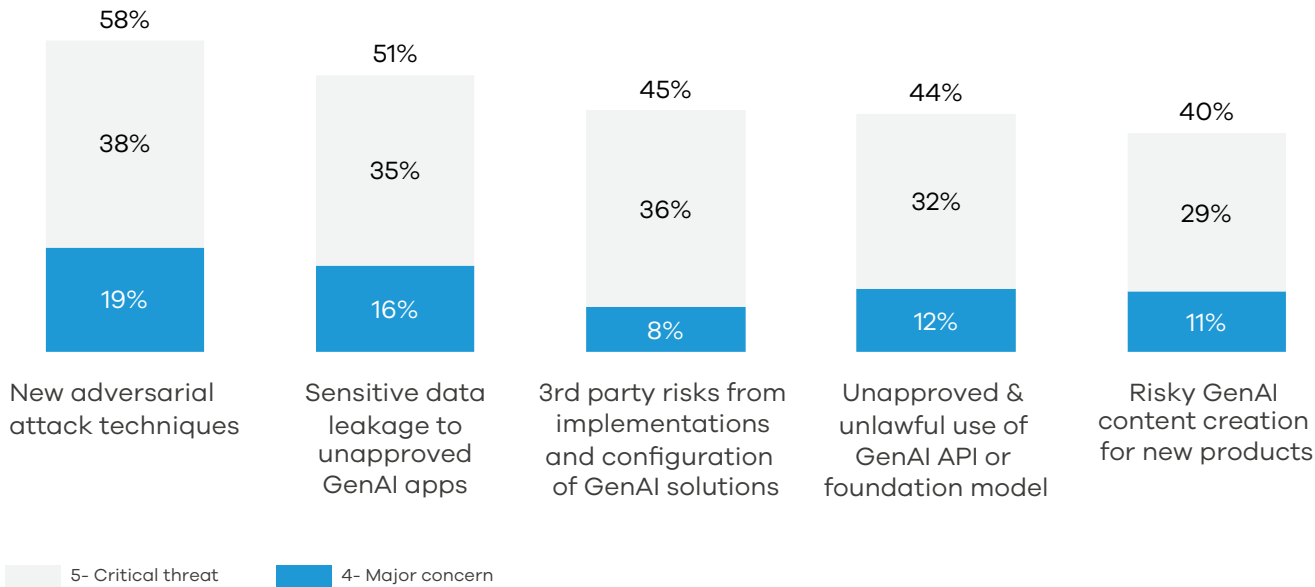
Our survey indicates that organizations leveraging GenAI effectively could see up to a 30% increase in operational efficiency, freeing up human resources to focus on more complex and strategic security challenges. However, the same features that make GenAI a powerful defense tool also pose serious risks

when exploited by adversaries. According to the forthcoming 2024 BCG CISO survey, 58% of leaders are concerned about “New adversarial attack technologies,” (Exhibit 14) which is reflected in their spending and posture for the coming year.

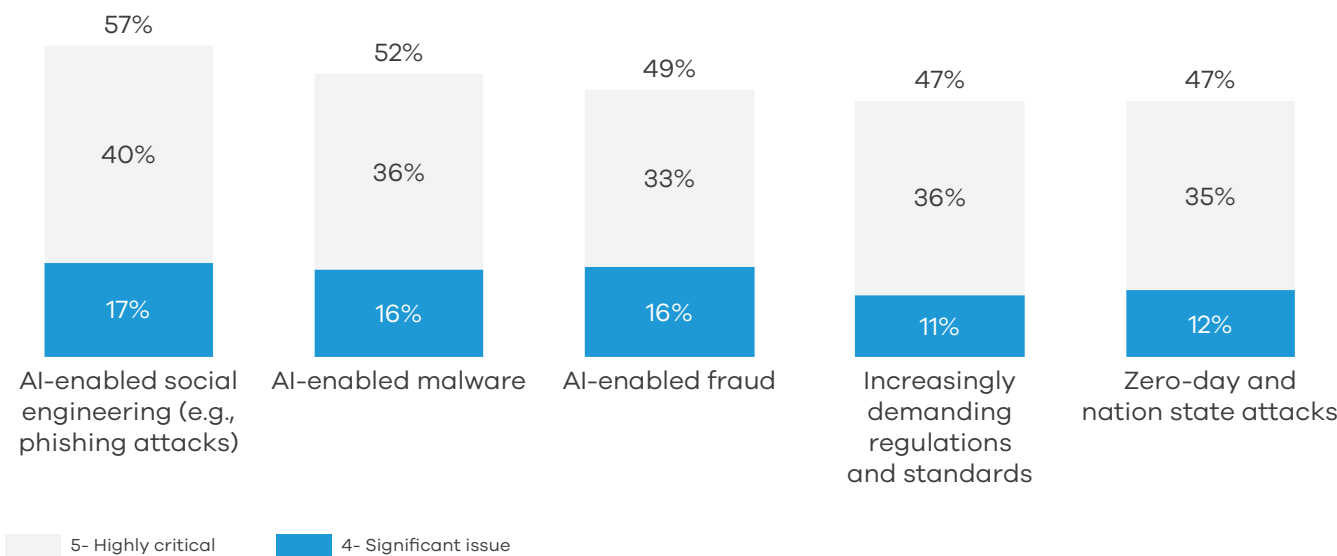
Exhibit 14 – New adversarial attack technologies

Major and critical GenAI threats

Q: On a scale from 1-5, please rate your concern with regards to the following GenAI threats.



Q: On a scale from 1-5, please indicate the importance of each driver on your cybersecurity posture and spend over the next year.



Source: BCG & GLG 2024 CISO Survey



04.

**SHAPING THE CYBER
WORKFORCE OF TOMORROW**

The rapid evolution of technology is both a blessing and a curse for organizations. Our survey shows that 60% of organizations

identified rapidly changing technology as the most significant challenge to keeping their cybersecurity teams up-to-date and effective.

60%



Organizations identified **rapidly changing technology** as the most significant challenge to keep skills of cybersecurity teams up to date

In response, organizations are investing in continuous training as a key approach to narrow the cybersecurity skills gap. Survey results show that 60% of organizations view this ongoing training as an essential means to ensure that their workforce is prepared to defend against emerging threats and to maintain the efficacy of their cybersecurity teams.

- **Institutionalizing Continuous Learning:** Investing in a culture of continuous learning is becoming increasingly essential. More than half of all respondents stated that upskilling a future-ready workforce, particularly in cybersecurity, requires facilitating a culture of continuous learning rather than just occasional training. These organizations prioritize professional development by allowing time for learning during work hours (51%) and reimbursing expenses for third-party courses (50%). This approach keeps employees engaged, motivated, and better prepared to navigate the fast-evolving technological landscape. However, the approach of every organization to training varies widely. While 57% of organizations rely on external training providers, 55% have developed internal training programs.

- **Proactive Skill Mapping and Gap Analysis:** It is essential to regularly assess the skillsets of your cybersecurity teams against the latest threat trends and skills framework. This proactive approach enables organizations to identify and address skill gaps before they become critical vulnerabilities
- **A Certification Paradox is emerging:** Despite 91% of organizations believing that industry certifications are important for bridging the cybersecurity skills gap, only 43% offer certification sponsorship to their employees, revealing a significant disconnect between belief in continuous learning and action.

According to our research, organizations providing more learning initiatives tend to have higher workforce satisfaction. This indicates that investing in employees' growth has benefits beyond enhancing technical skills. A continuous learning approach keeps employees engaged, motivated, and better prepared to navigate the fast-evolving technological landscape.

How organizations are maintaining an up-to-date cybersecurity workforce

60%

Consider continuous training essential

57%

Offer external trainings

55%

Provide internal trainings



05.

**CALL TO ACTION:
A ROADMAP TO SUCCESS**



Exhibit 15 - The Cybersecurity Talent Framework



1 Targeted and Strategic Outreach	2 Fostering a Culture of Lifelong Learning
1 Embedding Cybersecurity into Organizational DNA	2 Integrating Cybersecurity Education from the Group Up
1 National & Academic Campaigns for Cybersecurity Careers	2 Evolving Curriculum to Meet Industry Needs
4 Building an Inclusive, Diverse, and Supportive Culture	3 Adopt Skill-Based Hiring Practices
4 Clear Career Progression and Development	3 Expanding the Talent Pool with Inclusive Practices

Supply Side Demand Side

To build a future-ready cybersecurity workforce, a comprehensive and collaborative effort across the entire cybersecurity ecosystem is essential. Our strategic recommendations span the entirety of the Cybersecurity Talent Framework. Based on our research, the following actions should be prioritized.

- **Targeted and Strategic Outreach:** Implement highly targeted recruitment initiatives aimed at underrepresented groups, particularly women, and other minorities, through deep collaborations with educational institutions, industry bodies, and community organizations. These partnerships should go beyond surface-level engagement to include scholarships, mentorship programs, and dedicated career pathways that directly address the barriers these groups face in entering the cybersecurity field.
- **Embedding Cybersecurity into Organizational DNA:** Elevate cybersecurity roles within your organization's core strategy by branding them as essential to your mission and long-term success. Promote these roles not just as technical positions, but as critical to safeguarding global digital safety, thereby attracting mission-driven professionals motivated by purpose as much as by technical challenge.
- **National and Academic Campaigns for Cybersecurity Careers:** Collaborate with government bodies to launch national campaigns that position cybersecurity as a top career choice, featuring real-world case studies, role models, and interactive learning platforms. Academic institutions should work closely with the industry to provide real-time career guidance, ensuring that students understand the diverse and dynamic opportunities within the cybersecurity sector. This includes expanding access to internships, apprenticeships, and early-career experiences that seamlessly transition students into the workforce. Additionally, academic institutions should work with industry to craft curriculum that corresponds to demand.
- **Integrating Cybersecurity Education from the Ground Up:** Drive integration of cybersecurity education into primary and secondary school curricula to cultivate early interest and foundational knowledge. This should be reinforced by hands-on projects, cybersecurity clubs, and partnerships with industry professionals who can provide real-world context and mentorship.
- **Evolving Curriculum to Meet Industry Needs:** Regularly update educational curricula to align with the rapidly evolving demands of the cybersecurity landscape. This includes embedding cybersecurity training across multiple disciplines—such as law, business, and engineering—to ensure that future professionals are well-rounded and capable of addressing the multifaceted challenges of cybersecurity.
- **Fostering a Culture of Lifelong Learning:** Establish continuous learning platforms within organizations that provide cybersecurity professionals with ongoing access to the latest knowledge, tools, and best practices. Leverage partnerships with industry leaders and educational providers to offer certifications, micro-credentials, and advanced training programs that keep your workforce ahead of emerging threats. Centralize these resources into an easily accessible, comprehensive training hub to support professionals at all career stages.

- **Adopt Skills-Based Hiring Practices:** Use cybersecurity skills frameworks—the NICE Cybersecurity Workforce Framework, ECSF, and the SCyWF¹⁴—to pinpoint the specific skills, competencies, and knowledge needed for prioritized cybersecurity jobs and roles.
- **Expanding the Talent Pool with Inclusive Practices:** Challenge the status quo by broadening recruitment efforts to include nontraditional candidates, focusing on aptitude and potential rather than just experience. This includes targeting women and other underrepresented groups for internships and entry-level positions, and committing to upskilling and reskilling as necessary. Such strategies can effectively bridge the workforce gap and infuse cybersecurity teams with fresh perspectives.
- **Building an Inclusive, Diverse, and Supportive Culture:** Implement comprehensive DEI strategies that go beyond policy to create a truly inclusive workplace culture. This includes leadership-driven initiatives to promote psychological safety, gender equity, wellbeing, and the establishment of networks and mentorship programs that support the retention and advancement of women and other underrepresented groups in cybersecurity.
- **Clear Career Progression and Development:** Develop transparent career development pathways that provide cybersecurity professionals with clear opportunities for growth, learning, and advancement. Incorporate continuous feedback mechanisms, professional development plans, and access to leadership training to enhance job satisfaction and reduce turnover, ensuring that your organization retains top talent in a highly competitive environment.



14. NCA developed the Saudi Cybersecurity Workforce Framework



06.

BUILDING THE NEXT GENERATION OF CYBER DEFENDERS

To tackle the global workforce shortage and skills gap challenge, collaboration between decision-makers in public and private organizations as well as the cybersecurity ecosystem is essential. Leaders must work together to inspire and develop the next generation of cyber defenders by improving education, raising awareness, and providing opportunities for underrepresented groups. This includes integrating cybersecurity into school curriculums, offering training and upskilling programs, fostering a diverse talent pipeline, and creating an inclusive environment. Prioritizing workforce development and staying ahead of the evolving threat landscape can ensure a secure digital future and continue to promote global economic and technological progress.

Leaving the cybersecurity workforce shortage and skills gap unaddressed could have significant implications that cascade into areas including global security, economic stability, and technological innovation. As cyberattacks grow in frequency and complexity, organizations could be left struggling to defend critical systems, leading to potential breaches that could disrupt industries, governments, and economies. The cost of inaction will not only be measured in financial losses but also in the erosion of trust in the digital systems that underpin our global economy.



07. METHODOLOGY



Our robust methodology ensures that this report presents accurate and actionable insights into the global cybersecurity workforce shortage and skills gap. Through a multi-layered approach, we have leveraged diverse data sources, rigorous modeling techniques, and expert validation to deliver findings with high level of confidence.

Data Collection

We employed a meticulous data collection process, encompassing extensive survey, advanced web scraping, and in-depth interviews with key cybersecurity and workforce experts. This study surveyed

6,000 respondents from 48 countries, ensuring a representative sample across different regions, economic contexts, and cybersecurity maturity levels.

- **Country Selection:** We prioritized countries based on their economic significance and cybersecurity maturity, ensuring a balanced representation across high, medium, and low cybersecurity maturity levels. This approach guarantees that the study's findings are globally relevant and reflect the nuanced challenges faced by different regions.

Exhibit 16 – Country-wise split of responses

Country-wise split of responses (n=6,000)

America			Europe			Asia Pacific			Africa		
Country		Responses	Country		Responses	Country		Responses	Country		Responses
	United States of America	7.9%		United Kingdom	6.7%		India	7.5%		South Africa	1.1%
	Brazil	4.2%		Italy	5.0%		China	4.2%		Algeria	0.8%
	Canada	4.2%		Germany	4.3%		Japan	4.2%		Cameroon	0.8%
	Mexico	3.7%		France	4.2%		Indonesia	3.8%		Egypt	0.8%
	Argentina	1.0%		Spain	4.2%		Philippines	3.3%		Ghana	0.8%
	Chile	0.8%		Turkey	2.2%		South Korea	2.5%		Kenya	0.8%
	Colombia	0.8%		Albania	0.8%		Singapore	2.0%		Morocco	0.8%
	Costa Rica	0.8%		Bulgaria	0.8%		Australia	1.3%		Mozambique	0.8%
	Cuba	0.8%		Czech Republic	0.8%		Azerbaijan	0.8%		Nigeria	0.8%
	Panama	0.8%		Ireland	0.8%		Saudi Arabia	0.8%		Tanzania	0.8%
	Paraguay	0.8%		Romania	0.8%		UAE	0.8%		Tunisia	0.8%
	Peru	0.8%		Switzerland	0.8%		New Zealand	0.5%		Uganda	0.8%

- **Sector Focus:** Our analysis zeroes in on ten priority sectors, chosen based on their criticality to the global economy and the potential economic impact of security breaches. This sectoral focus enables us to provide targeted recommendations for industries that are most vulnerable to cybersecurity threats.
- **Respondent Diversity:** To capture a wide range of perspectives, we ensured that over 70% of respondents were C-suite executives and key decision-makers. This high-level engagement provides insights that are both strategic and operationally relevant.

Data Analysis and Modeling

We developed two comprehensive and integrated models to capture both the demand and supply sides of the cybersecurity workforce. These models are designed to provide a granular understanding of workforce dynamics, tailored to the unique characteristics of different countries.

- **Demand Modeling:** We constructed a detailed demand model that segments the 48 sampled countries into five archetypes based on cyber maturity and macroeconomic indicators. This model accounts for industry-specific and company-size variations, providing an accurate estimate of the total cybersecurity workforce and shortage. The model

was then extrapolated globally using a sophisticated scaling method based on cybersecurity revenue, ensuring that our projections are both precise and globally relevant.

- **Supply Modeling:** Our supply model mirrors the demand model's structure, focusing on the inflow and outflow of cybersecurity professionals. It estimates the number of new entrants to the workforce, both from academia and lateral hires, as well as those exiting the workforce through retirement or career changes.

Wherever there was limited reliable data availability, anchor country (country with reliable secondary data sources) in each archetype was used to form proxies for the remaining countries in the archetype cluster.

Expert Validation and Iterative Refinement

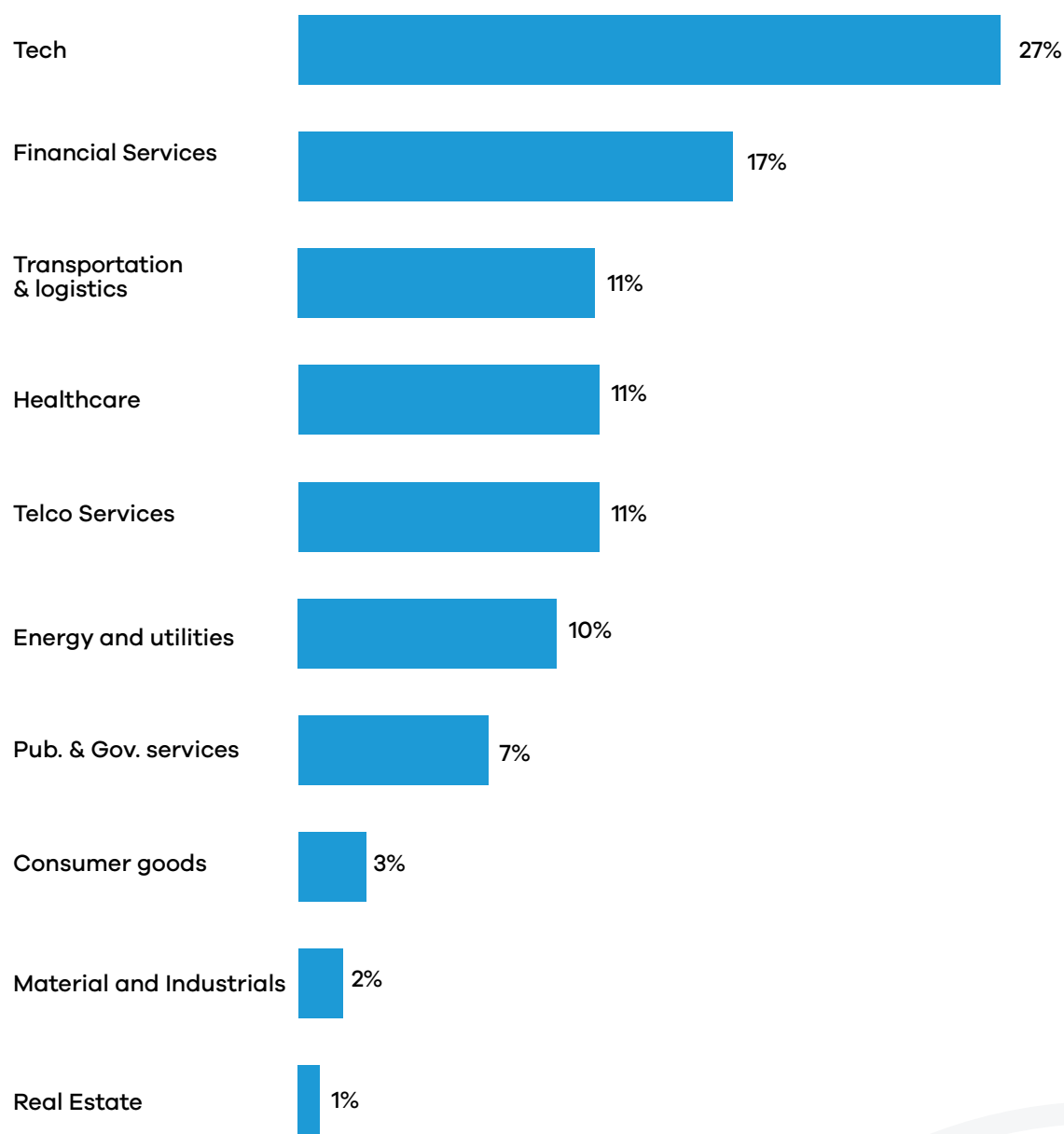
To ensure the robustness of our findings, we engaged in multiple rounds of expert discussions and iterative refinement. These discussions included cybersecurity leaders, academic researchers, and industry practitioners, who provided critical feedback that was incorporated into the final models. This collaborative approach not only strengthens the validity of our conclusions but also ensures that they are grounded in real-world challenges and opportunities.





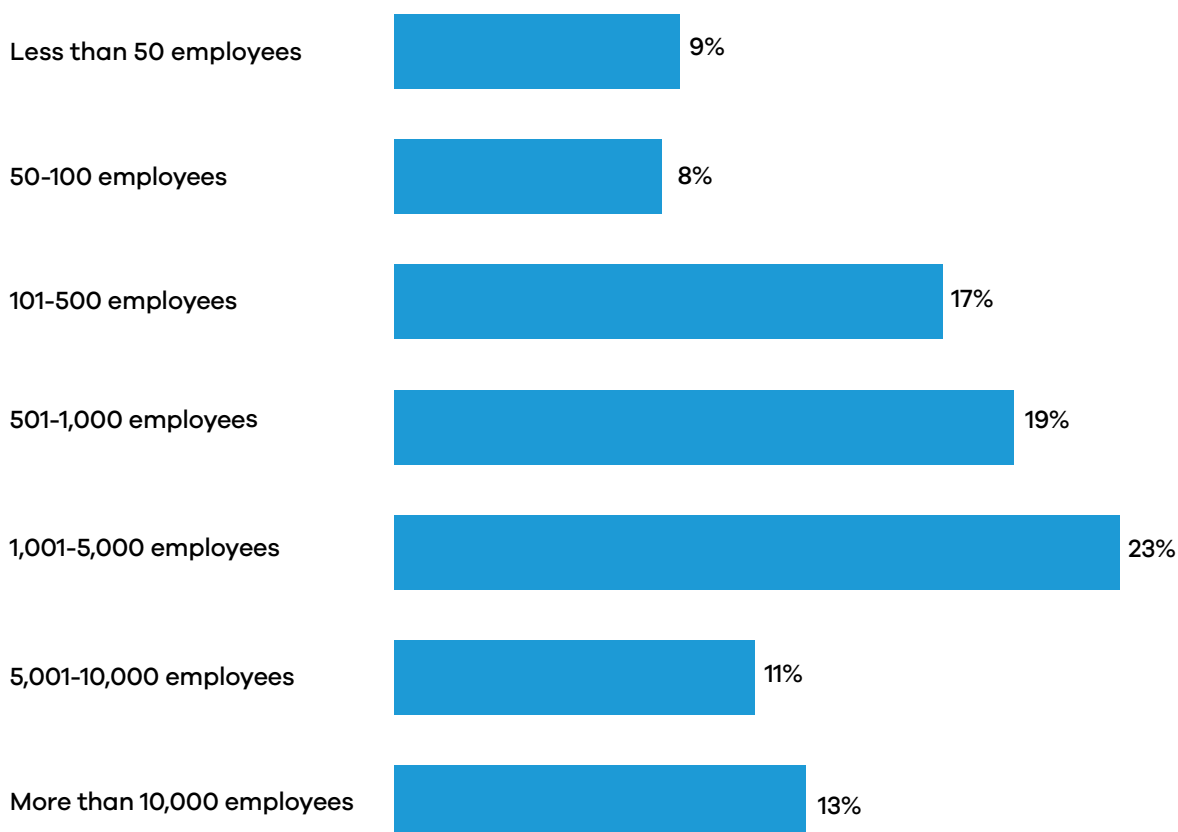
APPENDIX SURVEY DEMOGRAPHICS

Exhibit 17 - Survey respondents industry (n=6,000)



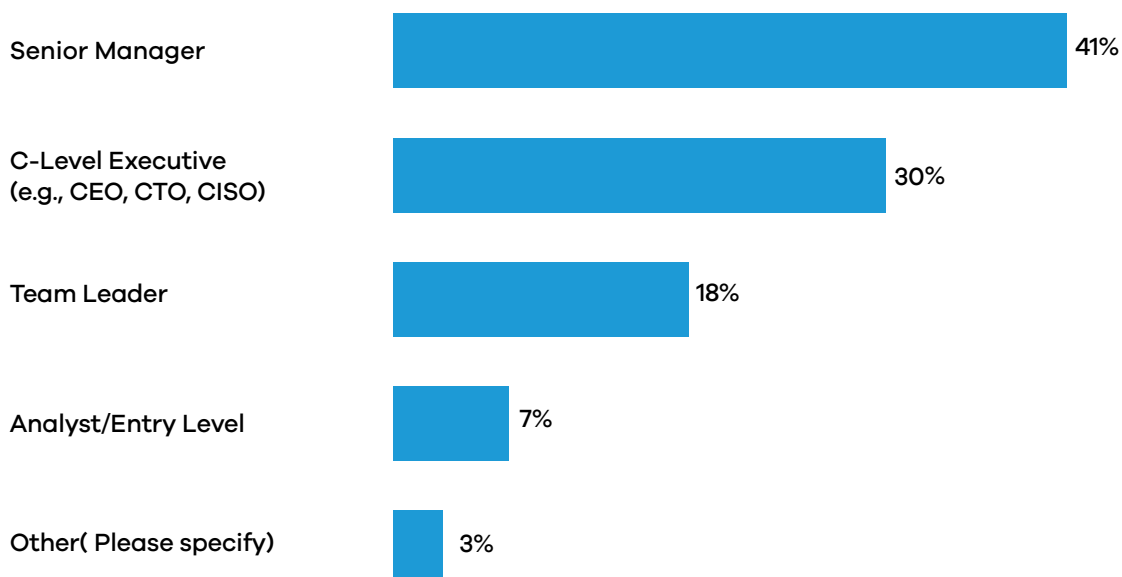
Source: Survey results

Exhibit 18 - Survey respondents company size (n=6,000)



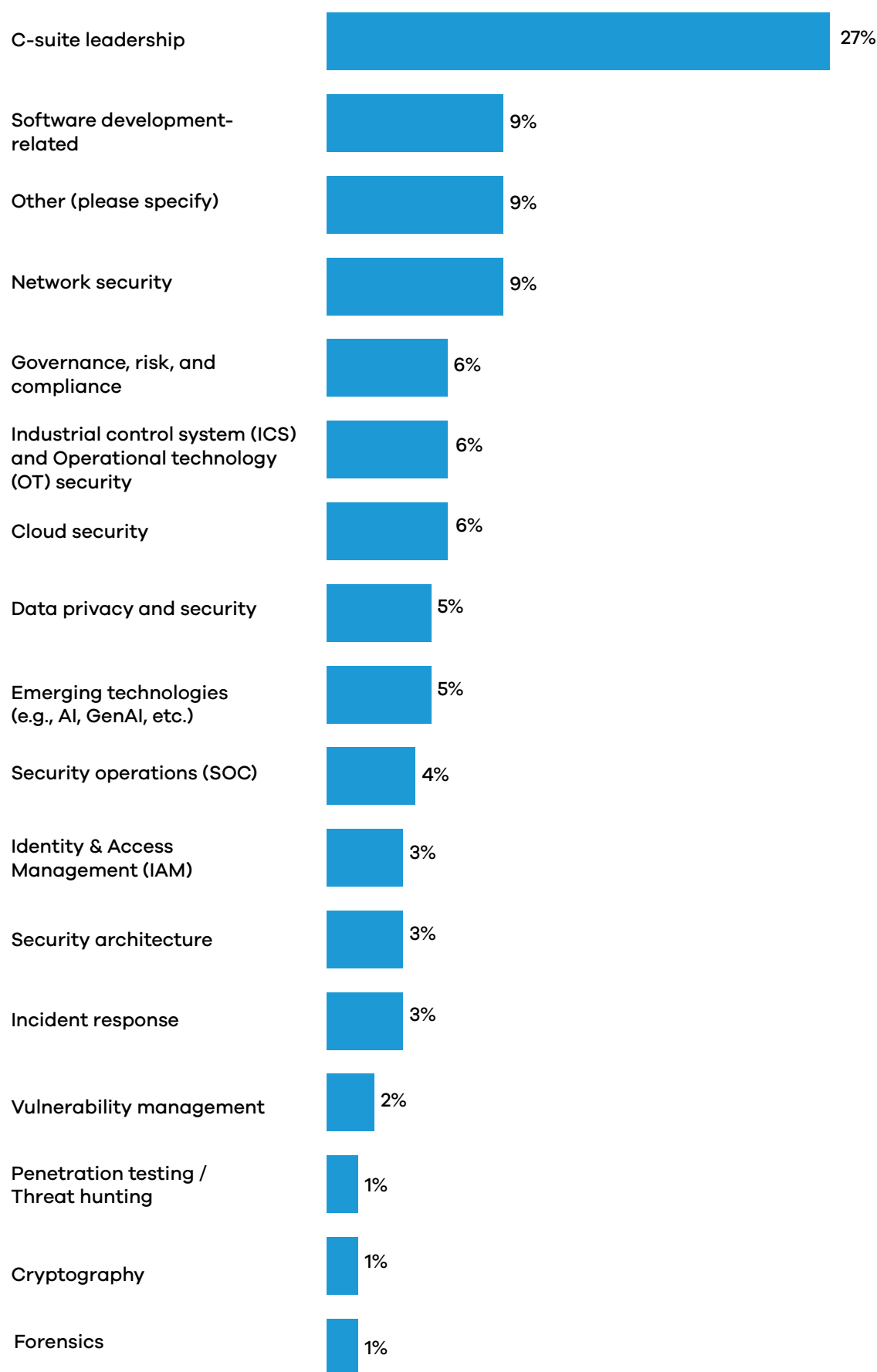
Source: Survey results

Exhibit 19 - Survey respondents seniority (n=6,000)



Source: Survey results

Exhibit 20 - Survey respondents role (n=6,000)



Source: Survey results





