ISC2 CYBERSECURITY WORKFORCE STUDY

ISC2™

Global Cybersecurity Workforce Prepares for an AI-Driven World

2024

Table of Contents

Executive Summary

Organizations have experienced a marked increase in risk and disruption in 2024. Economic pressures, exacerbated by geopolitical uncertainties, have led to budget and workforce reductions in a number of sectors, while cybersecurity threats and data security incidents have only continued to grow. Alongside these issues, organizations and professionals have had to keep pace with rapidly advancing technology innovations such as artificial intelligence (AI) in order to maintain and improve efficiency and agility. While the offer of transformative potential has fueled adoption, such technologies also introduce additional risks and exposure to regulation. Together, it has culminated in a year where resources are strained, impacting cybersecurity teams and their abilities to adopt new technologies and protect against the nuanced threats they pose to their organizations.

Each year, the ISC2 Cybersecurity Workforce Study assesses the state of the cybersecurity workforce to understand the composition of the talent and skills base, including looking at the size of the workforce and its shortages. We also look at the concerns of professionals in relation to their jobs, the cybersecurity and economic landscapes and the perceived cybersecurity needs of society from the perspective of those charged with protecting our digital world.

This year, we learned that the economic conditions have significantly impacted the workforce, leading to both talent shortages and skills gaps at a time when need has never been greater. At the same time, cybersecurity professionals are increasingly turning to AI, particularly generative AI (Gen AI), to help them drive transformation, cope with demand and shape strategic decisions within their organizations.

Hiring managers are prioritizing transferable skills that will complement AI adoption, such as problem-solving, over technical skills like cloud computing security or risk analysis. We found that while cybersecurity teams have ambitious plans for AI within the cybersecurity function, they anticipate the biggest return on investment will occur in two or more years. As a result, they are not immediately overhauling their practices to adopt AI. Cybersecurity professionals are also conscious of the additional risks AI will introduce across the organization. As different departments adopt AI tools, cybersecurity teams are encouraging their organizations to create comprehensive AI strategies.

For this report, ISC2 surveyed a record 15,852 international practitioners and decision-makers. These cybersecurity professionals span the globe from North America to Asia, Latin America, Europe, the Middle East and Africa. This report captures their perspectives and experiences, and it presents valuable findings to cybersecurity professionals and leaders, executives, policymakers, hiring managers and others to reveal solutions for the top challenges facing the workforce today.

Key Findings

Respondents don't believe their cybersecurity teams have sufficient numbers or the right range of skills to meet their goals. The state of the global economy has resulted in staff and budget reductions. We have seen an increase in the number of people needed globally to adequately secure organizations, yet employers are cutting back on hiring and the professional development of their cybersecurity teams. Almost 60% of respondents agree that skills gaps have significantly impacted their ability to secure the organization, with 58% stating it puts their organizations at a significant risk.

Participants' pathways to enter the cybersecurity workforce are changing, as are their priorities. Cybersecurity professionals are still focused on higher education and professional development once in the workforce, but they increasingly prioritize work-life balance (the top-ranked method of deriving meaning from their careers). The level of emphasis on different motivational factors varies across demographics, including tenure within their careers, though entrants to the field continue to trend older (39- to 49-year-olds).

Diverse backgrounds can help solve the talent gap. While IT is the traditional path into cybersecurity, more and more entrants come from different backgrounds or verticals. Respondents found these diverse pathways equally valuable to success in cybersecurity. With growing talent and skills shortages, it is smart for cyber teams to consider more backgrounds and professional experience to quickly fill gaps.

The expected advancements of AI will change the way cyber respondents view their skills shortage. AI will likely replace some of the technical skills needed in cybersecurity. While study participants speculated on what skills may be automated or streamlined, they cannot yet predict what activities, if any, AI will replace. As a result of this uncertainty, hiring managers aren't rushing to hire more specialized workers. Instead, they are prioritizing nontechnical skills like problem-solving that will be transferable through the increased use of AI.

Cyber professionals confident Gen AI will not replace their role. Only one-third of respondents are concerned about their role not being "future-proof" in a Gen AI world — the other two-thirds are confident that their expertise will complement the technology.

Gen AI presents benefits and challenges for cybersecurity. 45% of cybersecurity teams have implemented Gen AI into their teams' tools. They expect this implementation to bridge skills gaps, improve threat detection and provide vast benefits to cybersecurity. On the other hand, 64% of respondent organizations have implemented Gen AI in other departments, causing more work for cyber professionals. Over half have already faced data privacy and security concerns due to organizational adoption of Gen AI.

Organizations need a Gen AI strategy to responsibly implement the technology. As the adoption of Gen AI in cybersecurity continues to grow, cybersecurity professionals recognize the need for a formal strategy and regulations to govern its safe and responsible use. Nearly half of respondents report that their organizations currently lack a clear Gen AI strategy. And although 90% of respondents have some policies related to Gen AI, 65% say their organization needs to implement more regulations on the safe use of Gen AI.

Economic Conditions Create Resource Shortages

Challenging economic conditions led to increased resource reductions in cybersecurity. In 2024, 25% of respondents reported layoffs in their cybersecurity departments, a 3% rise from 2023, while 37% faced budget cuts, a 7% rise from 2023. These cuts have immense impacts on cybersecurity teams' ability to secure the organization.

- **Respondents say they don't have the staff they need to meet their goals.** 67% of respondents indicated they had a staffing shortage this year. Layoffs and budget cuts exacerbate security team shortages, which participants have told us are a persistent issue every year of this study. This has huge implications, as respondents say that a worker shortage was their biggest challenge over the past 12 months, and they predict a worker shortage will continue to be a significant challenge over the next two years.

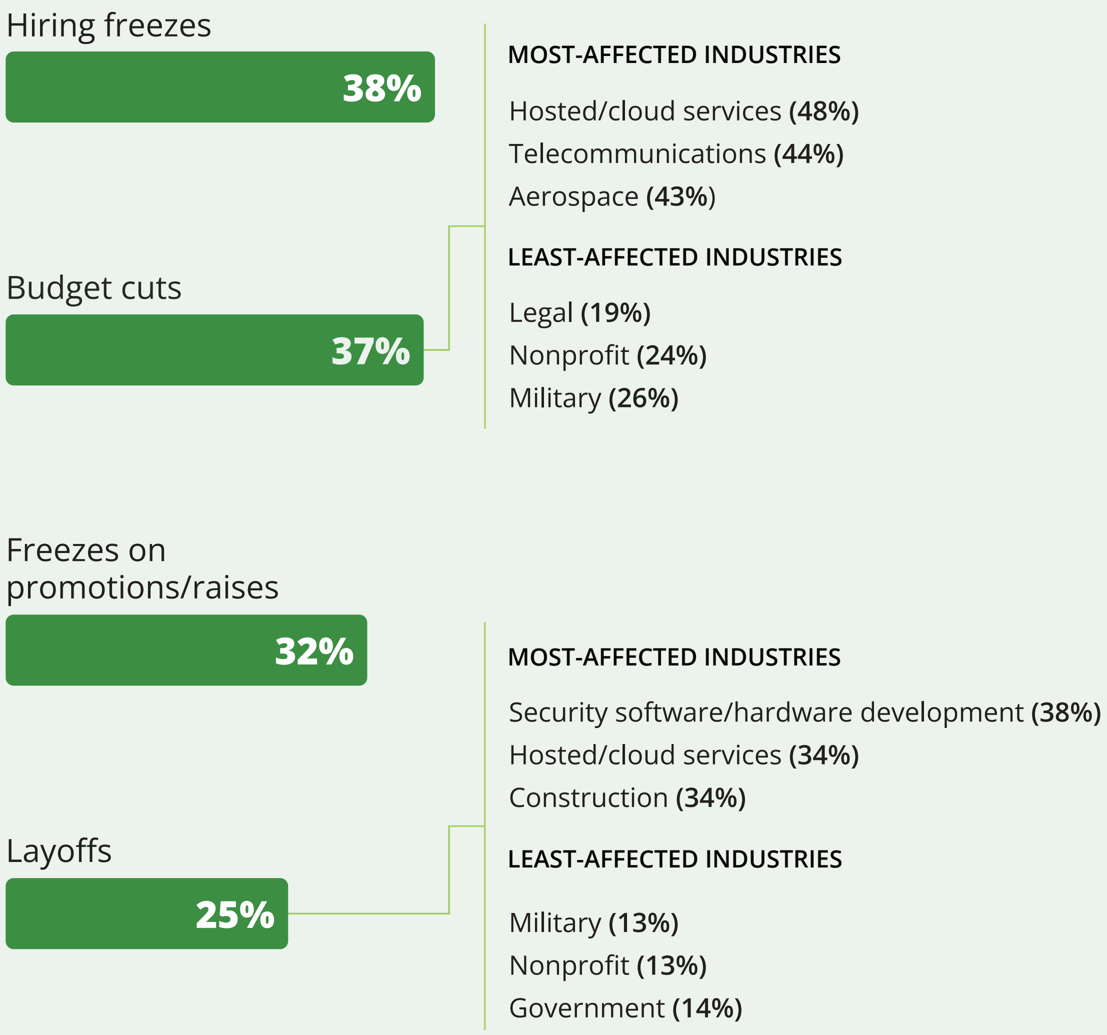
A lack of skills was the most challenging aspect of respondents' jobs over the past 12 months.

Workforce Insights

Hosted/cloud services, telecommunications and aerospace were the top three industries affected by cybersecurity budget cuts this year. On the other hand, public sector roles, nonprofits, military and legal were least affected by cybersecurity budget cuts (see Figure 1).

FIGURE 1

Has the cybersecurity team in your organization experienced the following cutbacks in the past 12 months?



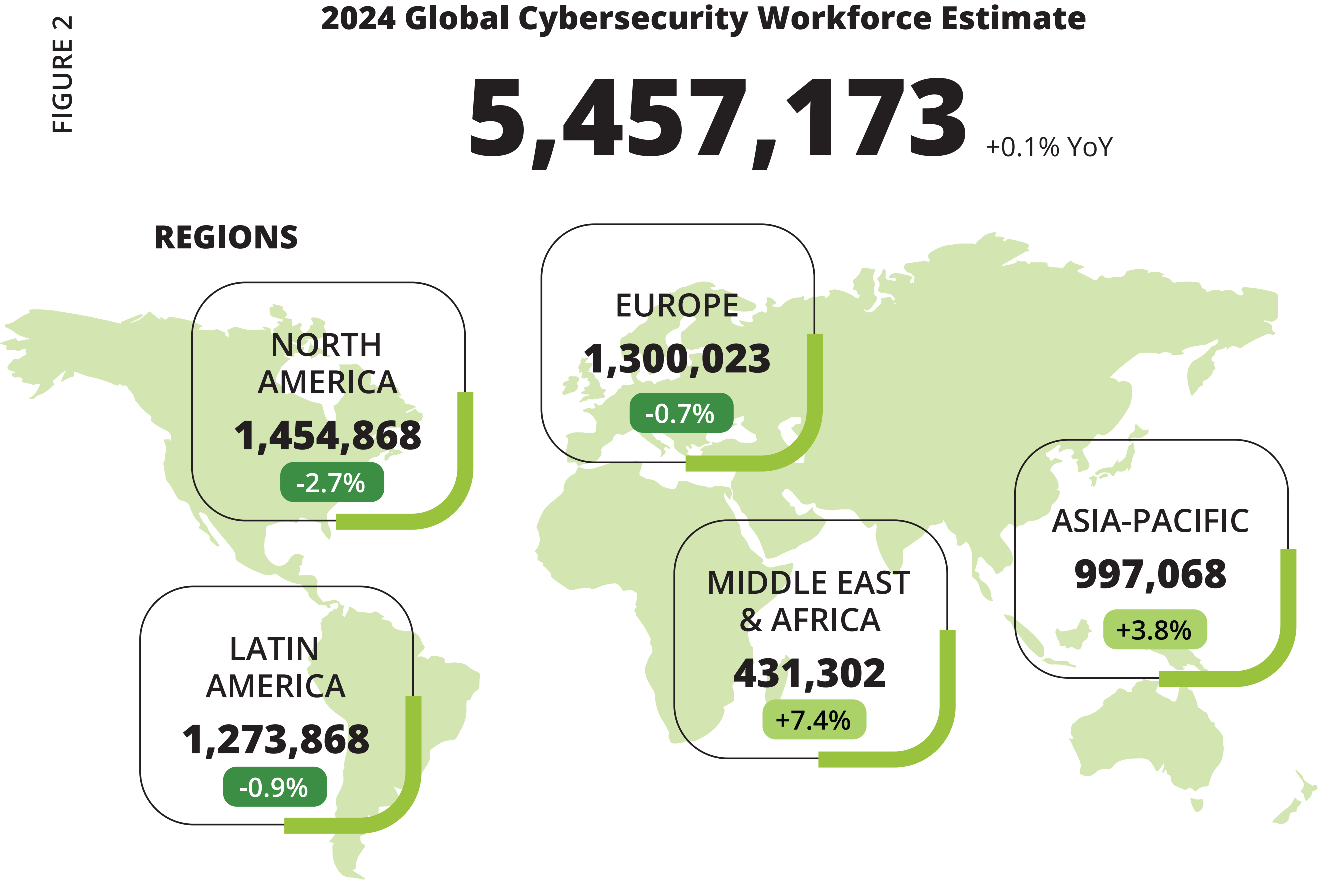
Base: 12,069 global cybersecurity professionals

To better understand the workforce gap, we first need to understand the size of the cybersecurity workforce. Because no global resource tracks this, we have developed an estimation methodology. This proprietary methodology leverages a wide array of primary and secondary data sources to extrapolate the number of workers responsible for securing their organizations (see Appendix A for details). We estimate the cybersecurity global workforce to be 5,468,173 employees. This is a 0.1% increase from 2023. This change resulted from growth in the Middle East and Africa (7.4%), and Asia-Pacific (3.8%). This growth was countered by reductions across Europe (-0.7%), North America (-2.7%) and Latin America (-0.9%) cybersecurity workforces (see Figure 2).

Even with increases in certain regions, the cybersecurity workforce growth is slowing — there was an 8.7% workforce increase between 2022 and 2023 with every region adding to their ranks. This year's numbers suggest that hiring has slowed for 2023–2024.

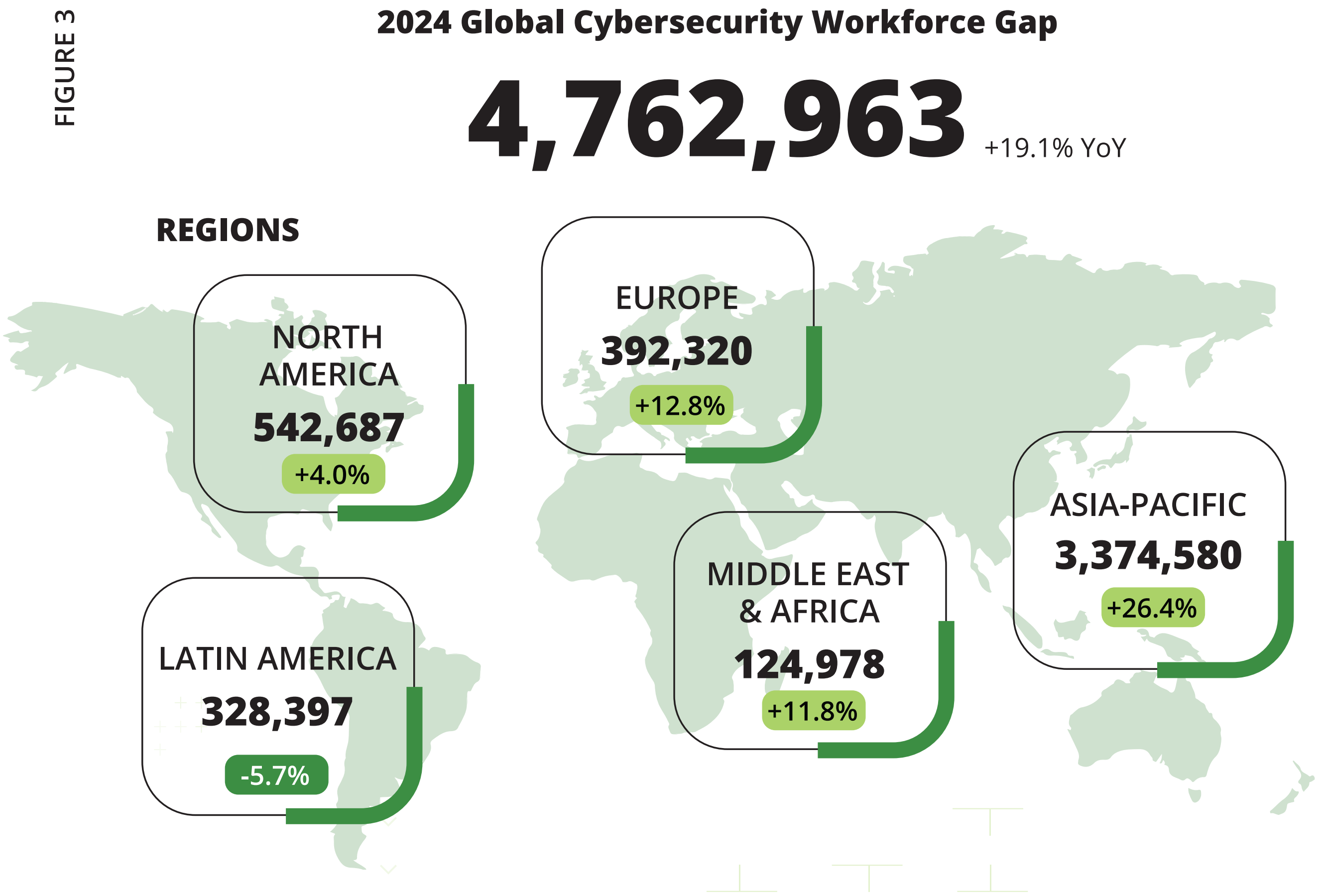
FIGURE 2

2024 Global Cybersecurity Workforce Estimate



Our workforce gap estimate methodology considers the security team shortages, as reported by our study participants, and the staff needed to adequately keep their organizations secure. It also incorporates the workforce size estimate previously mentioned and other primary and secondary data sources. This year, the workforce gap was 4,763,963 people. (For more information about ISC2's workforce gap estimate methodology, see Appendix B.) This is a 19.1% increase from 2023, with the greatest rise in Asia-Pacific and Europe (see Figure 3).

FIGURE 3



The workforce gap measures the difference between the number of cybersecurity professionals that study participants say their organizations require to properly secure themselves and the number of active cybersecurity professionals. It is not an estimate of current job openings for cybersecurity professionals.

- **Skills shortages make it difficult to secure the organization.** 64% of respondents believe that skills gaps (see Figure 6 for examples) can have a more significant negative impact than a staffing shortage. Cybersecurity professionals are feeling this pressure, as 90% of respondents have one or more skills gaps on their cybersecurity teams.
- **Lack of budget is the main cause for talent shortages and skills gaps.** Respondents indicated the number one cause for both their talent and skills gaps is budget (see Figure 4). In 2023, the top causes for talent and skills gaps were an inability to find the talent or skills they needed to succeed. But today, it's not just about supply, it's also about limited resources for hiring and skills development, which illustrates how the economy is affecting the cyber workforce. More than a quarter (26%) highlighted the challenges of retaining people with in-demand skills, while 22% are struggling with developing and advancing their cybersecurity staff. These challenges are expected to persist, as nearly 20% of respondents also expect more cybersecurity layoffs in the next 12 months.

For more insights into the slowing growth of the global cybersecurity workforce, read ***Employers Must Act as Cybersecurity Workforce Growth Stalls and Workforce Skills Gaps Widen***.

FIGURE 4

You indicated your organization has one or more skills gaps. What do you think are the biggest causes of these gaps?

(Showing top five responses)

33%

My organization doesn't have the budget to hire enough people

30%

My organization can't find people to hire with the skills we need

27%

In general, we struggle to keep people with in-demand skills

27%

My organization has gaps in emerging technology areas

26%

IT often introduces new tech but doesn't have the expertise to secure it

Base: 12,069 global cybersecurity professionals

You indicated that your organization has a shortage of cybersecurity staff. What do you think is the biggest cause for this shortage?

(Showing top five responses)

39%

My organization doesn't have the budget

35%

My organization can't find enough qualified talent

28%

My organization doesn't pay a competitive wage

23%

My organization is struggling to keep up with turnover/attrition

22%

My organization can't offer opportunities for growth/promotion for security staff

Base: 6,270 global cybersecurity professionals

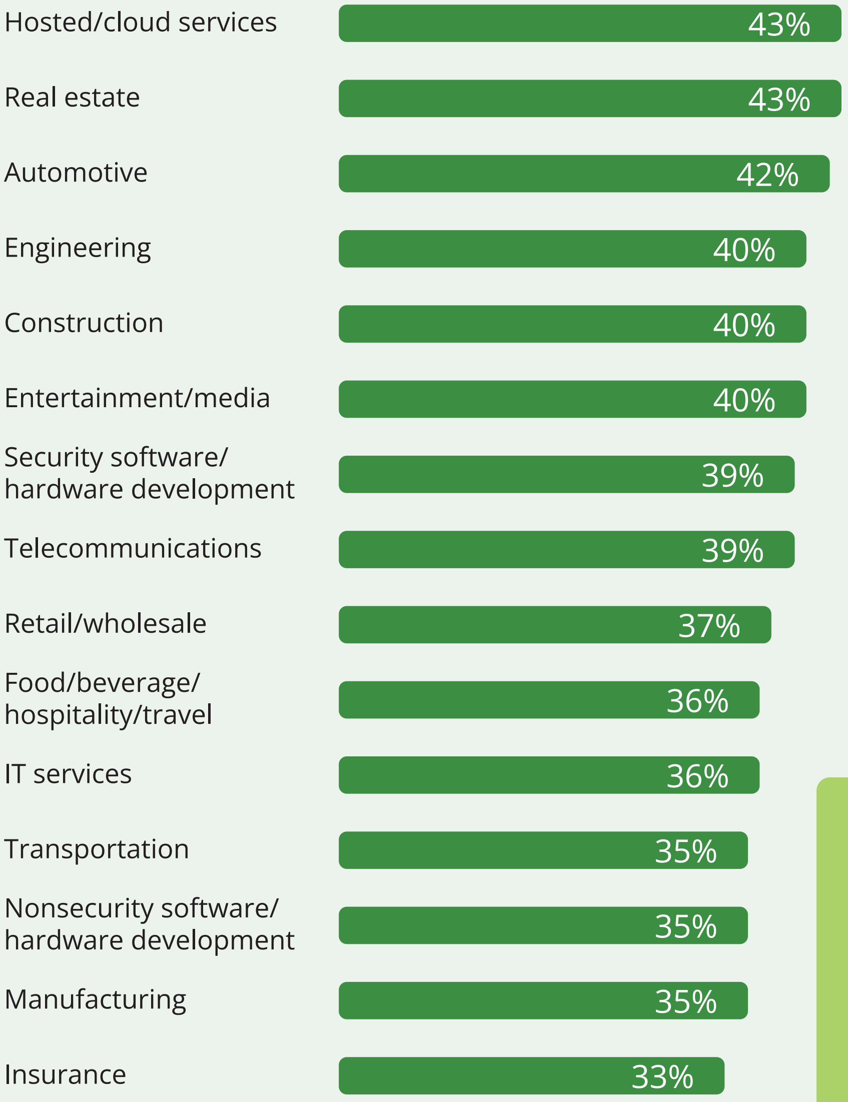
Workforce Insights

Hosted/cloud services (43%), real estate (43%), automotive (42%), engineering (40%), construction (40%), entertainment/media (40%), security software (39%) and telecommunications (39%) are anticipating more cybersecurity cutbacks over the next 12 months (see Figure 5). Public sector industries, including military (16%), government (24%) and utilities (25%), expect lower rates of cybersecurity cutbacks in the future.

FIGURE 5

We expect there to be cutbacks in cybersecurity over the next 12 months at my organization.

(Showing "Somewhat agree/Completely agree" responses)



Base: 12,069 global cybersecurity professionals
Note: Showing top 15 industries

Expect Cutbacks

Average across all industries:

31%

- **Lack of time is a secondary cause for the skills gap.** Cybersecurity professionals are working as hard as they can to meet their job requirements. In an ideal world, workers would learn new skills to stay current with the market, but more than half of respondents reported they don't have enough time to learn new skills.
- **The skills gap significantly impacts organizational security.** 59% of respondents agree that skills gaps have substantially affected their ability to secure their organizations, with 58% stating it puts their organizations at a significant risk. Further, organizations with critical or significant skills gaps are almost twice as likely to experience a material breach compared to organizations with no skills gaps. Of the nearly 7,500 participants who were willing to share information about material breaches, 17% said their organization experienced a breach last year. When we segment that by organizations with skills gaps, we see that 22% experienced a material breach last year.

Deep Dive on Needed Skills

Cloud computing is the most desired skill. Hiring managers and non-hiring managers state cloud computing security is the top technical skill needed, remaining consistent from 2023. Hiring managers are seeking candidates who are experienced in:

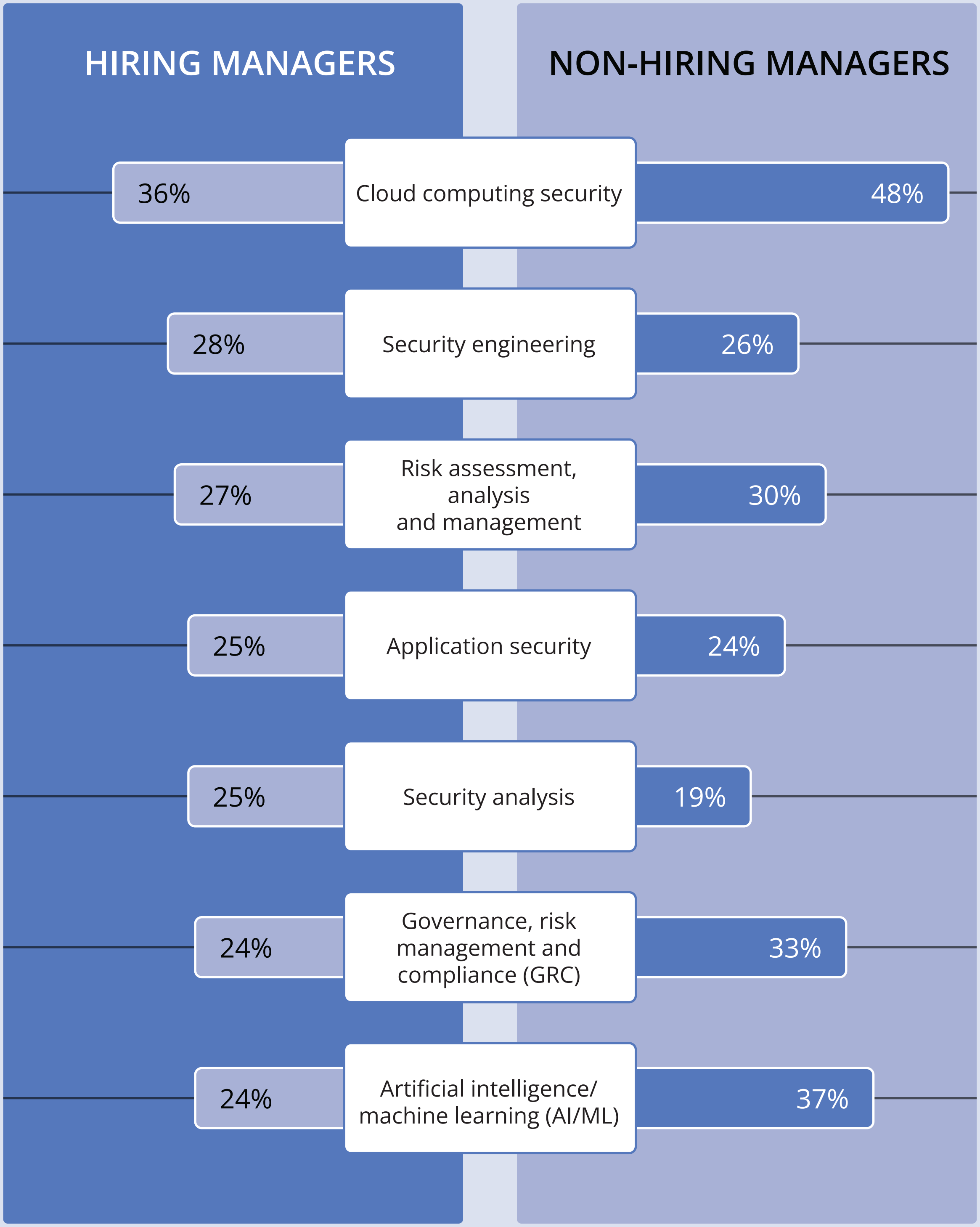
- Cloud platform and infrastructure security
- Cloud data security
- Cloud architecture and design

AI was the second most desired technical skill among non-hiring managers (see Figure 6). Hiring managers are focused on skills that can provide immediate benefits and see AI as a future benefit. This may explain why skills like security engineering and risk assessment analysis rank above AI.

FIGURE 6

What technical skills are you most looking for right now when hiring?

What technical skills do you think are most in demand for security professionals looking to advance their careers?



Base: 7,698 global cybersecurity professionals

Base: 8,154 global cybersecurity professionals

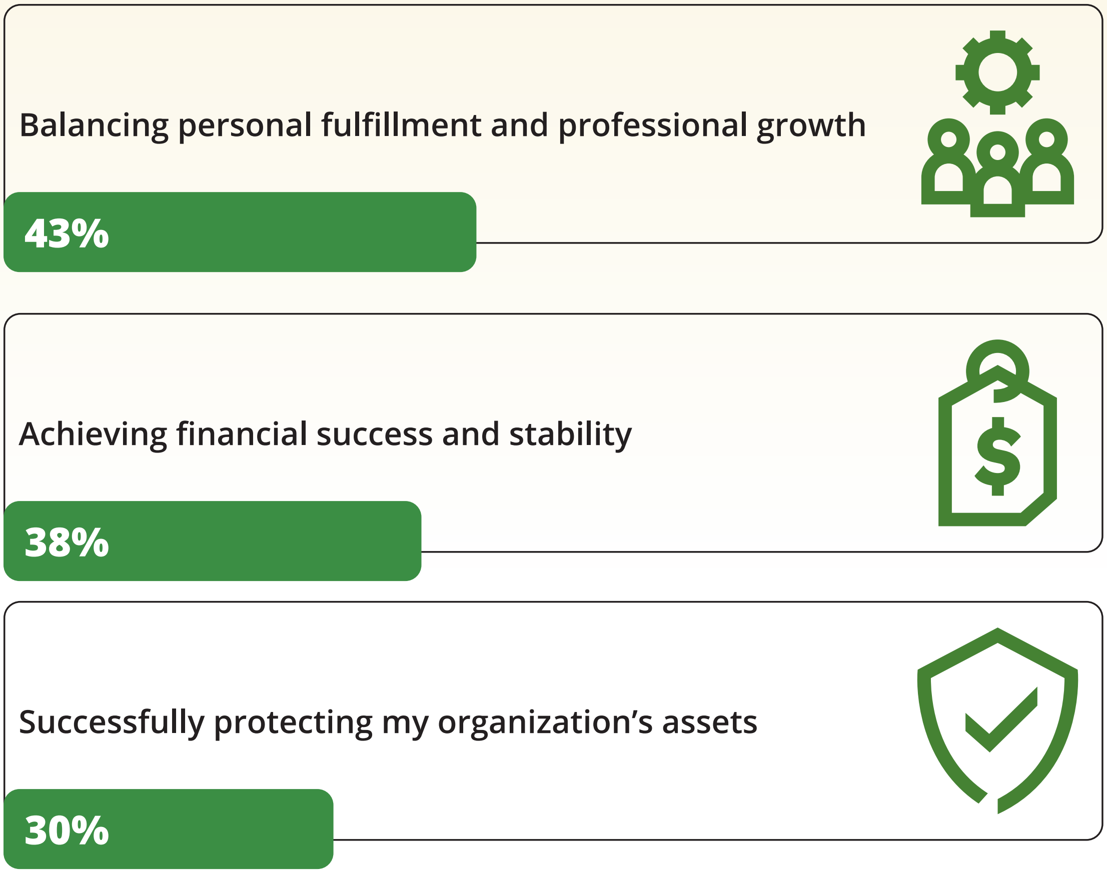
Cybersecurity Career Growth Aspirations and Pathways

Cybersecurity professionals are feeling the repercussions from their organizations' budget cuts and layoffs, even if they are not directly affected. Employees do not expect promotions and instead are prioritizing work-life balance (see Figure 7). But this doesn't mean that cybersecurity professionals are less committed to the mission. They still want to make sure they help protect their organizations. While they are motivated to protect critical assets and perform their primary function, they are also hopeful for future career advancements within AI.

FIGURE 7

Rank the following in terms of how meaningful they would be (or already are) for you to achieve in your cybersecurity career.

(Showing top three responses)



Base: 15,852 global cybersecurity professionals

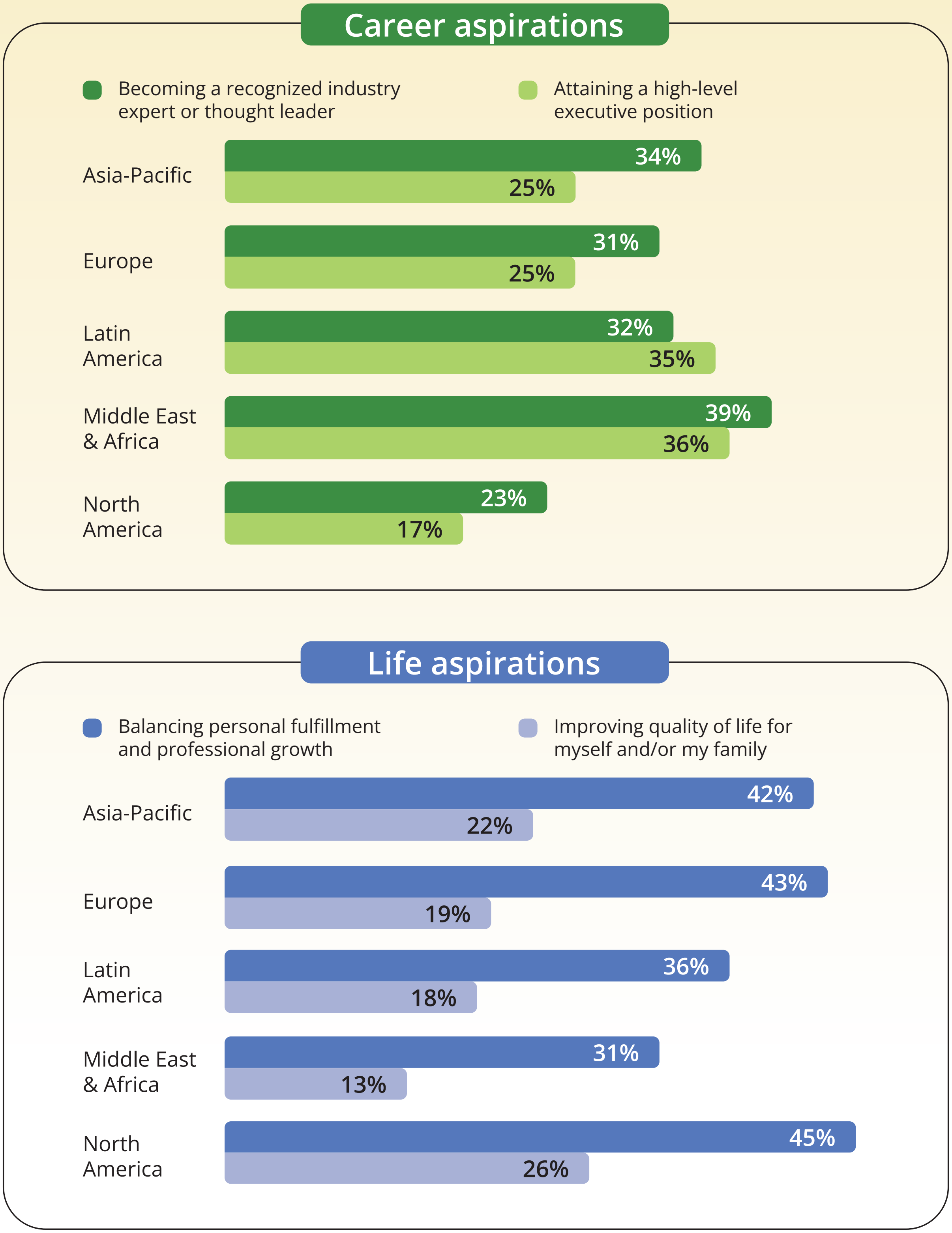
- **Cybersecurity professionals' motivations differ across demographics.**

  Regional: While cyber professionals' top career goal overall is to balance personal fulfillment and professional growth, this sentiment is most prevalent in North America (45%), Europe (43%) and Asia-Pacific (42%), while less popular in Latin America and the Middle East and Africa (see Figure 8). North Americans are also focused on improving the quality of life for themselves and their families (26%), more so than Europe, Latin America or the Middle East and Africa, all with percentages below 20%. Latin America and the Middle East and Africa are more focused on the professional aim to attain a high-level executive position (35% and 36%, respectively) or become a recognized industry expert or thought leader (32% and 39%, respectively). Asia-Pacific shares the thought leader drive at 34% (see Figure 8). One item to note: Work-life balance might be a generational value, as older employees are more focused on securing their company than on their personal fulfillment.

FIGURE 8

Rank the following in terms of how meaningful they would be (or already are) for you to achieve in your cybersecurity career.

(Showing top three rank percentage)



Base: 15,852 global cybersecurity professionals
Note: Showing 4 of 11 response options.

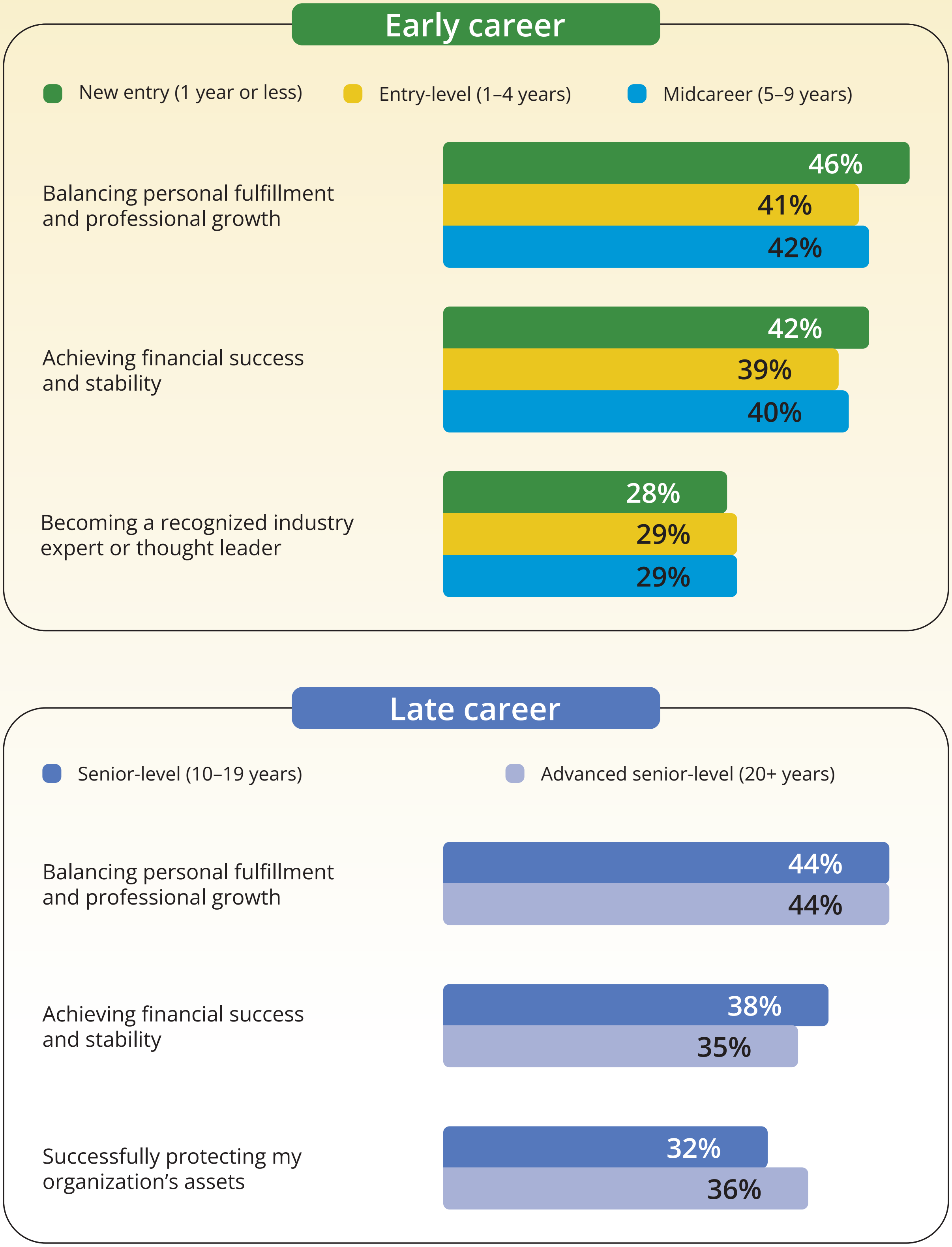
Tenure: Motivations also differ based on cybersecurity career tenure. New-entry workers (with tenure of one year or less) find the most meaning in balancing personal fulfillment and professional growth (46%) while also achieving financial success and stability (42%). Entry-level workers also chose those as top priorities, but with less enthusiasm (41% and 39%, respectively). While balancing their personal and professional lives remains the top priority, the numbers for success and stability reduce with tenure. In contrast, factors such as successfully protecting their organization's assets climbs as tenure increases, ranked by 36% of advanced senior-level (with 20 or more years' experience) workers. As workers gain their footing within the industry, their motivation for personal gain is balanced with the desire to maintain the security of their organization (see Figure 9).

- **Cybersecurity professionals are realistic about near-term career advancement.** On average, most professionals believe they are at the right level in the organization. This belief combined with the possibility of future resource cutbacks mean the majority of professionals don't have immediate aspirations toward a promotion. 18% of respondents completely agreed they are actively looking for a new cybersecurity job right now, while 25% completely disagreed. When asked to place themselves on a spectrum of their desire to become a manager to remaining as an individual contributor, their responses were neutral. On a similar spectrum, respondents were neutral in their interest to become a CISO (see Figure 10).

FIGURE 9

Rank the following in terms of how meaningful they would be (or already are) for you to achieve in your cybersecurity career.

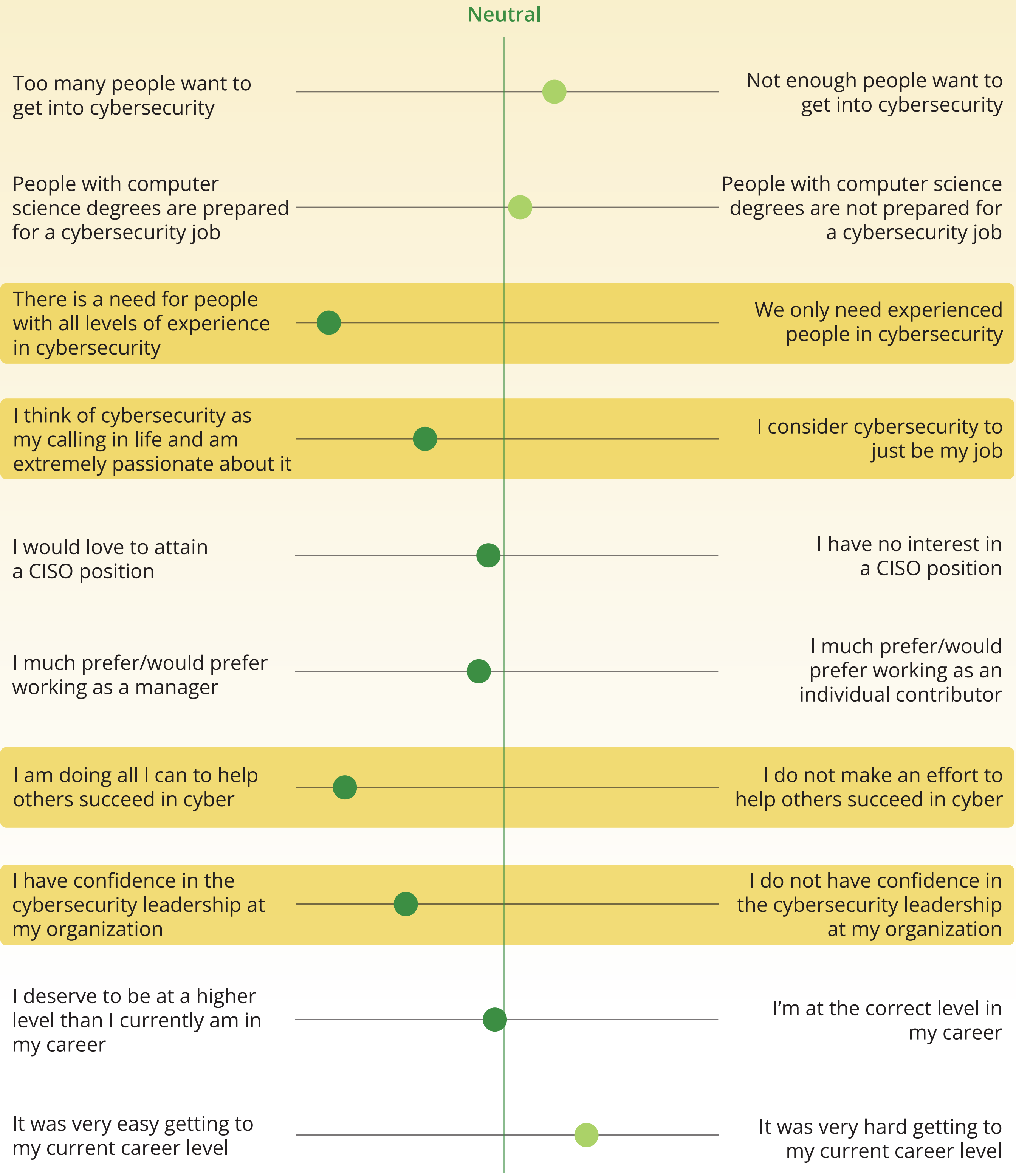
(Showing top three ranked responses)



Base: 15,852 global cybersecurity professionals

FIGURE 10

In your opinion, where do you land in each of the following scales in terms of your cybersecurity career and cybersecurity careers in general?



Base: 15,852 global cybersecurity professionals

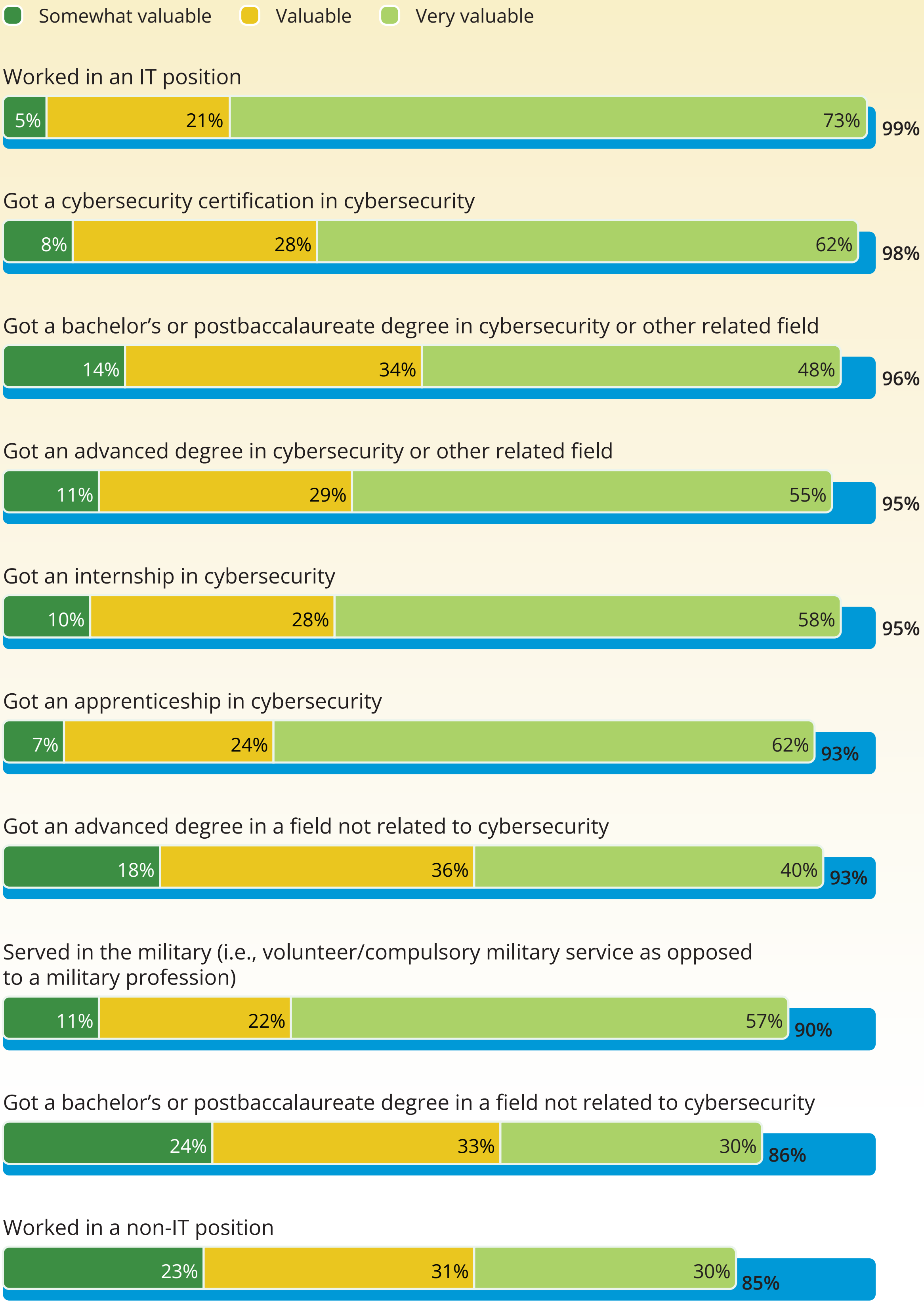
Diverse Pathways and Certifications Can Lead to Successful Careers

IT continues to be the most popular pathway into cybersecurity (70%); however, the manner in which workers find their way into cybersecurity is slowly diversifying. While education (cybersecurity-related or not) is still a common pathway into cybersecurity — with 62% of respondents entering the cybersecurity workforce directly from higher learning institutions — 18% previously worked in a non-IT position. Embracing this diversity of entry pathways could potentially mitigate the workforce gap by supplying a more diverse knowledge base into the workforce.

- **Diverse backgrounds can help solve the talent gap.** While IT is the traditional path into cybersecurity, more and more new entrants come from different backgrounds. Professionals found these diverse pathways equally conducive to success in cybersecurity (see Figure 11). With the growing talent gap, cyber teams must look to all backgrounds to fill gaps. Whether they are coming from an area outside of IT or lacking a degree, workers acknowledge that professional development and certifications can help upskill once they are in the role.

FIGURE 11

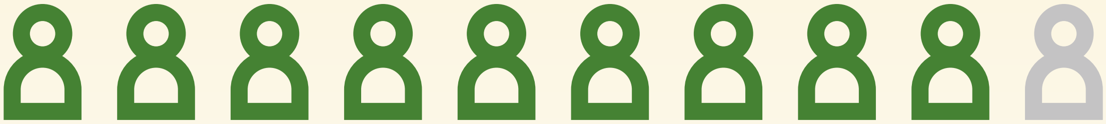
How valuable have you found each of the following in your career growth in cybersecurity?



Base: 306 to 11,056 global cybersecurity professionals
Note: Individual percentage values may not sum to totals due to rounding.

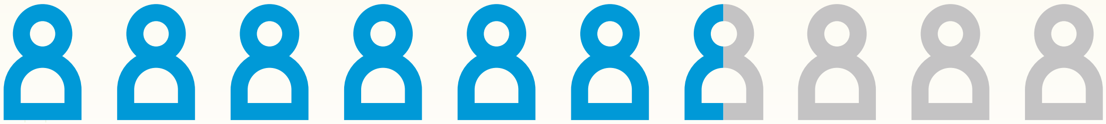
- **Certifications enable employees with an array of backgrounds.** Certifications have proven to be a popular and effective way to bolster internal expertise — 86% of professionals said they value their cybersecurity certifications; those who got a cybersecurity certification before their first job in cybersecurity found it valuable or very valuable (90%). Another 65% say certifications are the best way to prove knowledge and understanding (see Figure 12). This remains true across regions, gender and race, underscoring certification's significance for demonstrating cybersecurity skills, regardless of background.

FIGURE 12



90% **of respondents who got a cybersecurity certification before their first job in cybersecurity found it valuable or very valuable for their career.**

Base: 2,511 global cybersecurity professionals who got a certification before their first job in the field



65% **of respondents somewhat or completely agree that cybersecurity certifications are the best way to prove knowledge and understanding of concepts.**

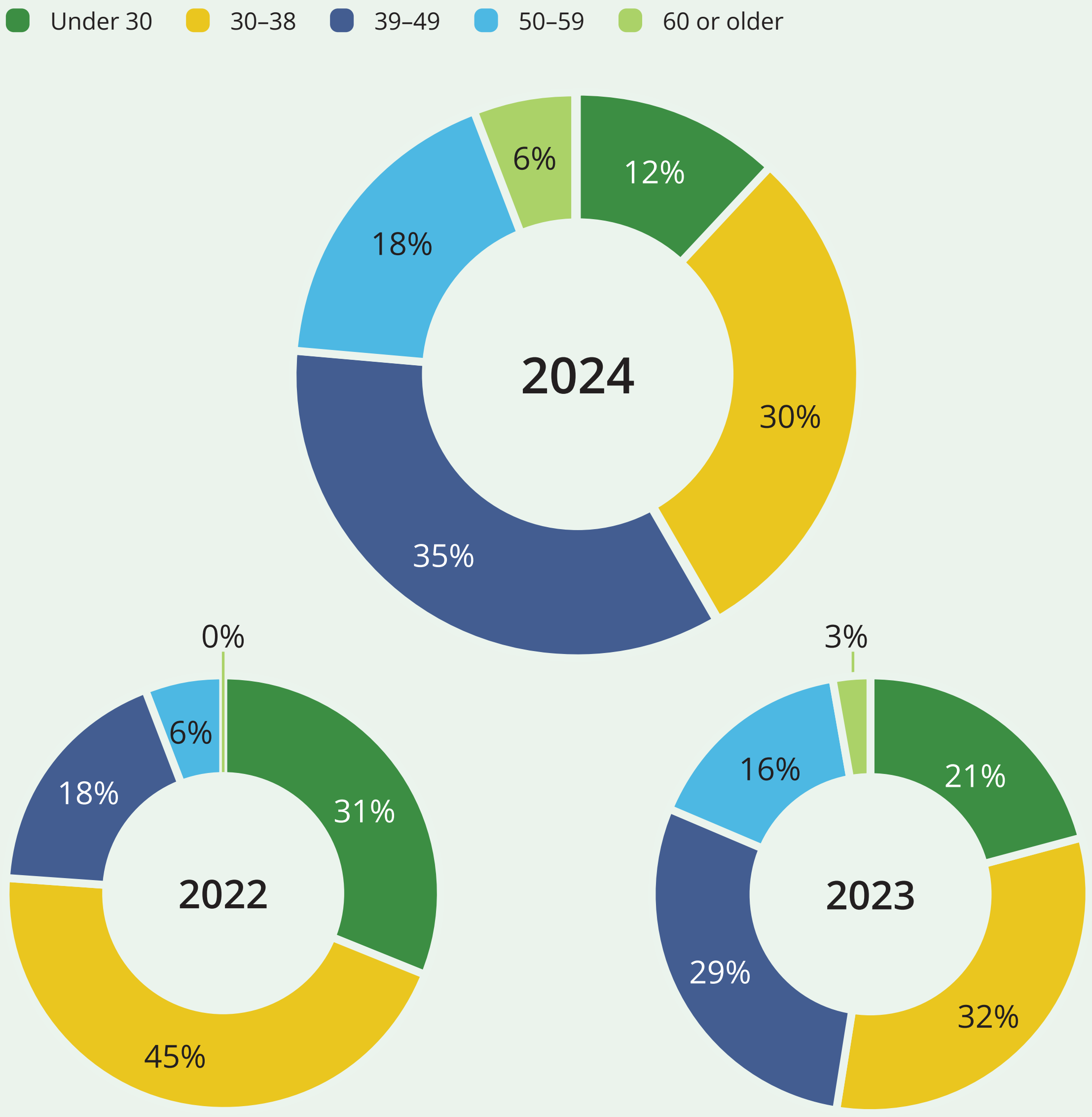
Base: 15,744 global cybersecurity professionals

Workforce Insights

Of survey participants entering the cybersecurity profession within the past year, there has been an increase in 39- to 49-year-olds, which has continued to rise, year-over-year, from 18% in 2022 to 35% in 2024 (see Figure 13).

FIGURE 13

Ages of new entrants into the cybersecurity profession (i.e., started in cybersecurity within the last year).



Base: 488 global cybersecurity professionals who started in the past 12 months
695 surveyed in 2023; 356 surveyed in 2022
Note: Individual percentage values may not sum to totals due to rounding.

Respondents Are Changing Their Skills Approach to Prepare for an AI-Driven World

The expected advancements of AI have changed the way professionals view their skills shortages. In the past, they were keen to adopt niche technical skills, but AI is a game changer for two main reasons. First, experts predict AI will be able to replace some of the technical skills needed in cybersecurity. Second, and arguably more important, no one is certain how AI will manifest in cybersecurity since they currently cannot predict what skills, if any, it will replace. As a result of this uncertainty, hiring managers aren't rushing to hire more specialized workers. Instead, they are prioritizing nontechnical skills, like problem-solving, that will be transferable through the increased use of AI.

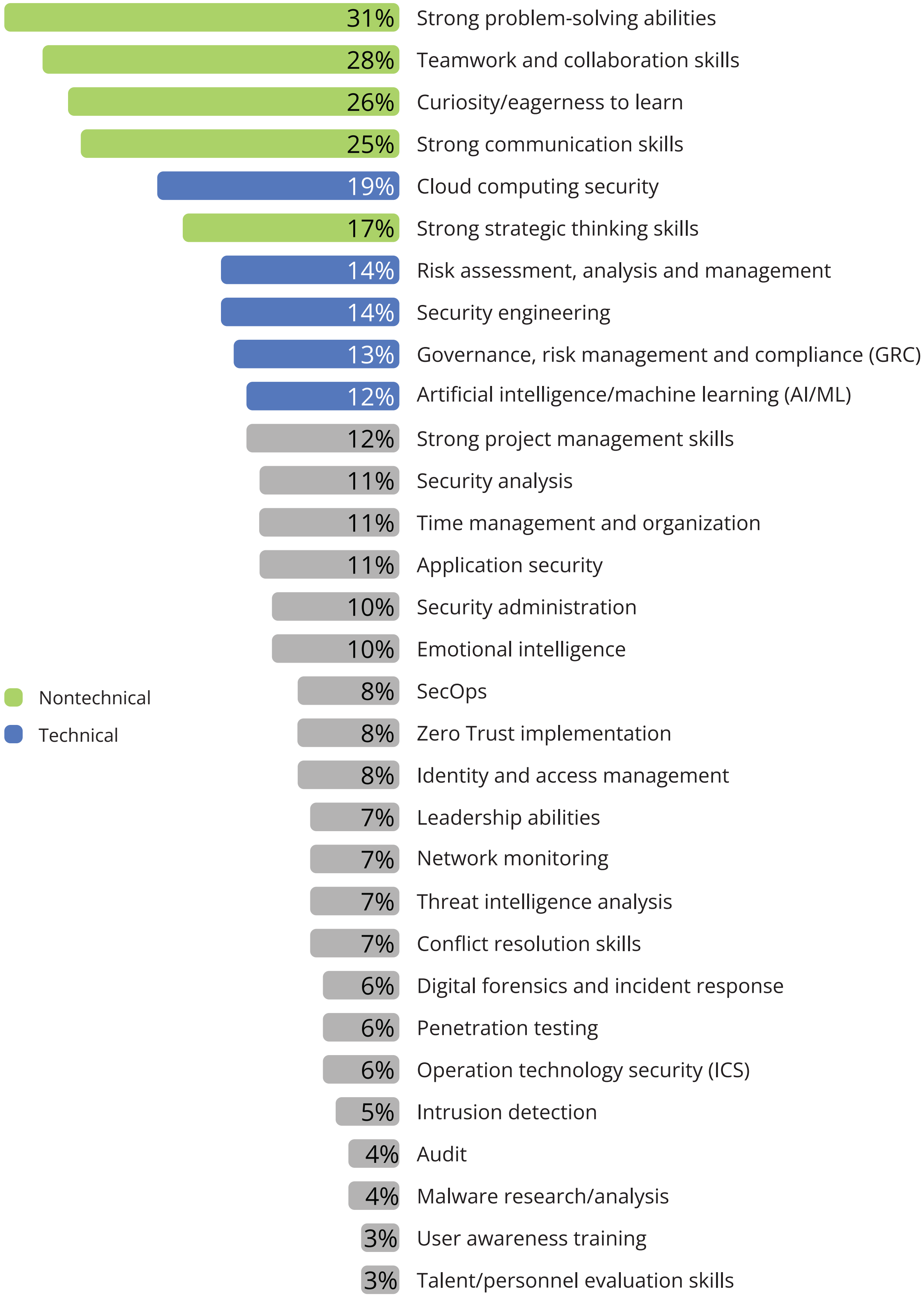
- **Nontechnical skills are viewed as more transferable as people adapt to an AI world.** Professionals understand that the future is AI; however, 59% of hiring managers don't know enough about Gen AI to know which skills professionals will need to succeed in an AI-driven world. As a result, hiring managers are not betting on specialized technical skills because they may or may not provide benefit in the future. Instead, hiring managers seem to favor nontechnical skills that will be transferable no matter what the future looks like.

  The top skills hiring managers are looking for today are strong problem-solving, teamwork, collaboration, curiosity and communication. These skills ranked higher than technical skills like cloud computing security, risk assessment, analysis and management and AI (see Figure 14).

  Non-hiring managers also see the value of nontechnical skills: the top skill they believe they need to advance their career is strong communication skills. However, non-hiring managers still place a high value on technical skills for advancement as they also believe cloud computing and AI are necessary for moving up (see Figure 15).

FIGURE 14

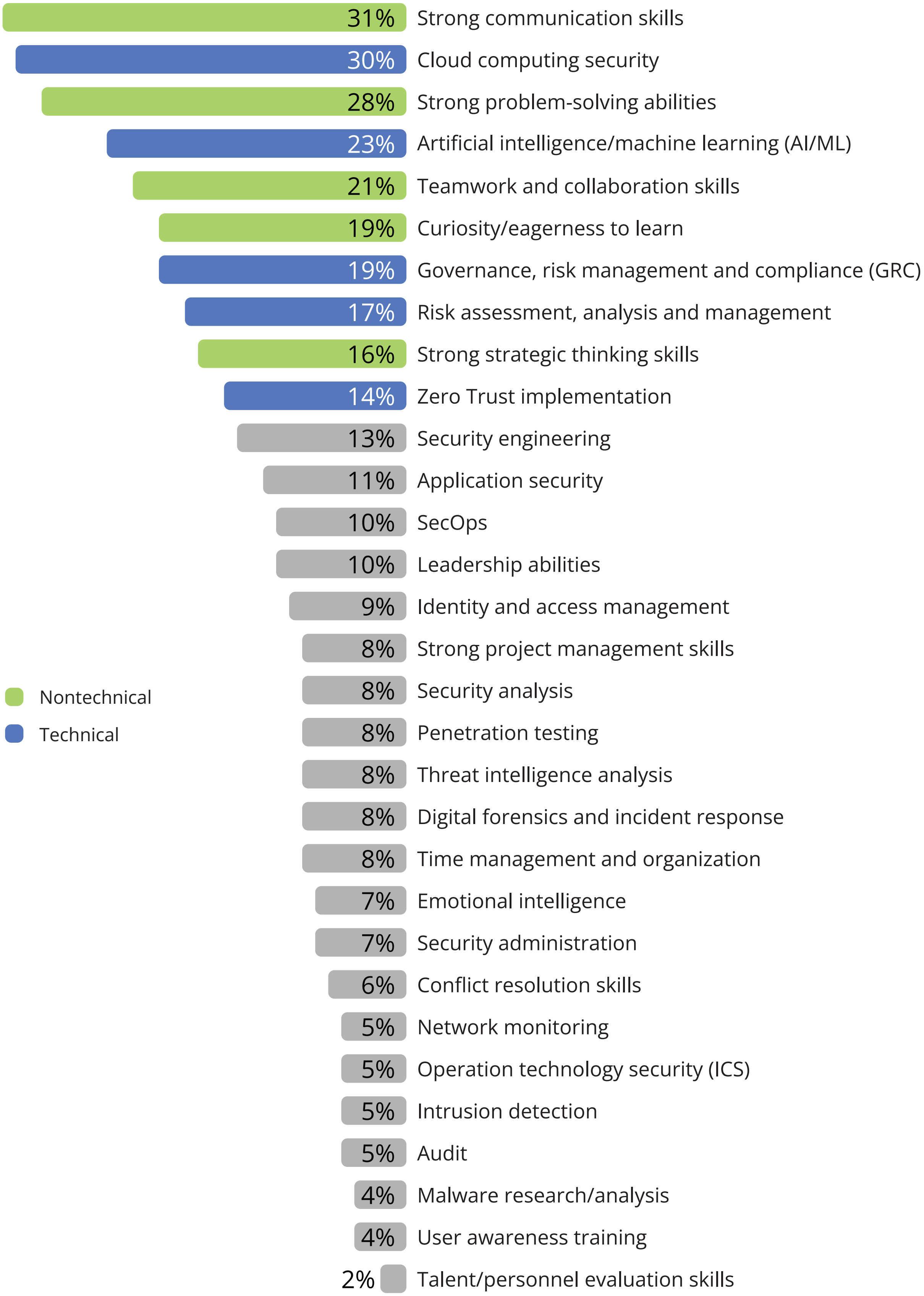
Among the technical and nontechnical skills you are looking for now as a hiring manager, what are you most looking for right now when hiring?



Base: 7,698 global cybersecurity professionals with hiring authority
Note: Asked to hiring managers

FIGURE 15

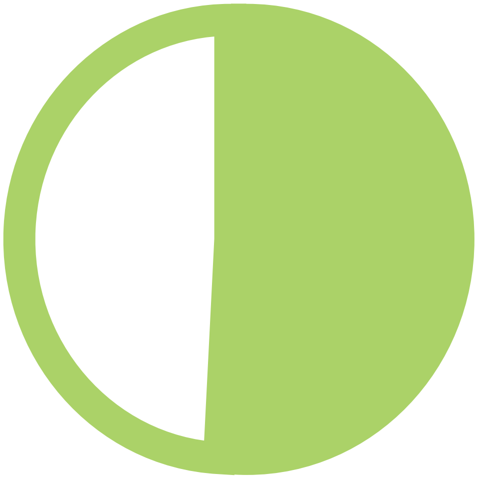
Among the following technical and nontechnical skills, what do you as a non-hiring manager believe are most in demand for cybersecurity professionals looking to advance their careers (via new jobs and promotions)?



Base: 8,154 global cybersecurity professionals
Note: Asked to non-hiring managers

- **AI may assume some cybersecurity tasks, but it won't replace the human skill set.** As we move to a more automated world, cybersecurity professionals are anticipating what will be required of them. They predict skills like problem-solving and teamwork will be more valuable, and 51% said nontechnical skills will be more important for cyber professionals in an AI-driven world (see Figure 16).

FIGURE 16



51%

of respondents somewhat or completely agree that nontechnical skills will be more important for cybersecurity professionals in an AI-driven world.

Base: 15,571 global cybersecurity professionals

Workforce Insights

When comparing regional data, North Americans are the least concerned about future-proofing for AI, while Latin America and the Middle East and Africa have higher levels of concern. However, Latin America and the Middle East and Africa are also most excited about career growth opportunities via AI.

Deep Dive:
Cyber Professionals’ Sentiment Around AI

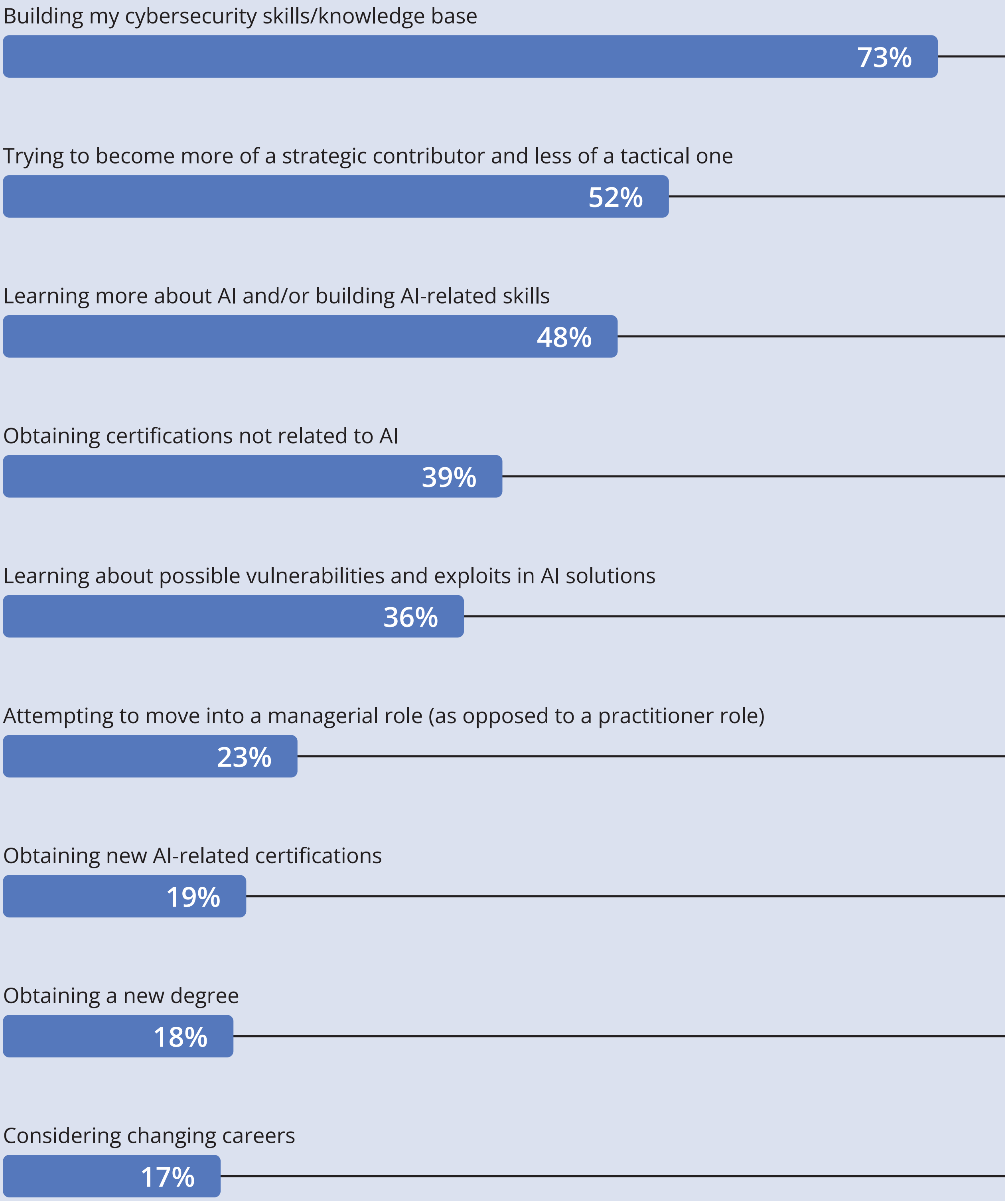
Cybersecurity professionals are worried AI will replace some of their job responsibilities; however, they don’t believe the technology can replace their entire role. With this mindset, professionals are taking specific actions to prepare for AI and overall are excited for an AI future.

- **The uncertainty surrounding AI is encouraging Δj.** Cybersecurity professionals are aware of the potential impact of AI in their roles. They understand the technology has the ability to perform certain aspects of their job, and 51% believe Gen AI, specifically, will result in certain cybersecurity skills becoming obsolete. In response, cyber professionals want to make themselves more future-proof for a Gen AI-driven world. To do so, 73% of professionals are building their cybersecurity skill set, 52% are focused on becoming a more strategic contributor and 48% are learning more AI-related skills (see Figure 17). It’s notable that professionals are taking a similar approach to hiring managers and are focusing on transferable skills, as 66% of professionals don’t know enough about Gen AI to know what skills they will need to learn to succeed in an AI-driven world.

FIGURE 17

What, if anything, are you doing to try to make yourself more future-proof in a more Gen AI-driven world?

(Showing “I am currently doing this/have already done it” responses)



Base: 6,762 to 15,575 global cybersecurity professionals

- **Most professionals are confident AI will complement their expertise.** Only one-third of professionals are concerned about their role not being future-proof in a Gen AI world — the other two-thirds are confident that their expertise will complement the technology.
- **Cyber professionals are embracing the potential benefits of AI.** Cyber professionals are generally excited about the potential of AI, with 54% saying it will be more helpful to cybersecurity as a whole.

  Further, they see personal advancement opportunities: 66% of professionals believe Gen AI presents a career growth opportunity for them personally, and 80% believe their cybersecurity skill set will be more important in an AI-driven world. Not only will AI bring more importance to the cybersecurity role, but 71% also believe Gen AI will allow them to do their job more efficiently.

The majority of professionals view Gen AI as a career growth opportunity.

Two Sides of the Same Coin: How AI Both Benefits and Increases Risks for Cybersecurity Teams

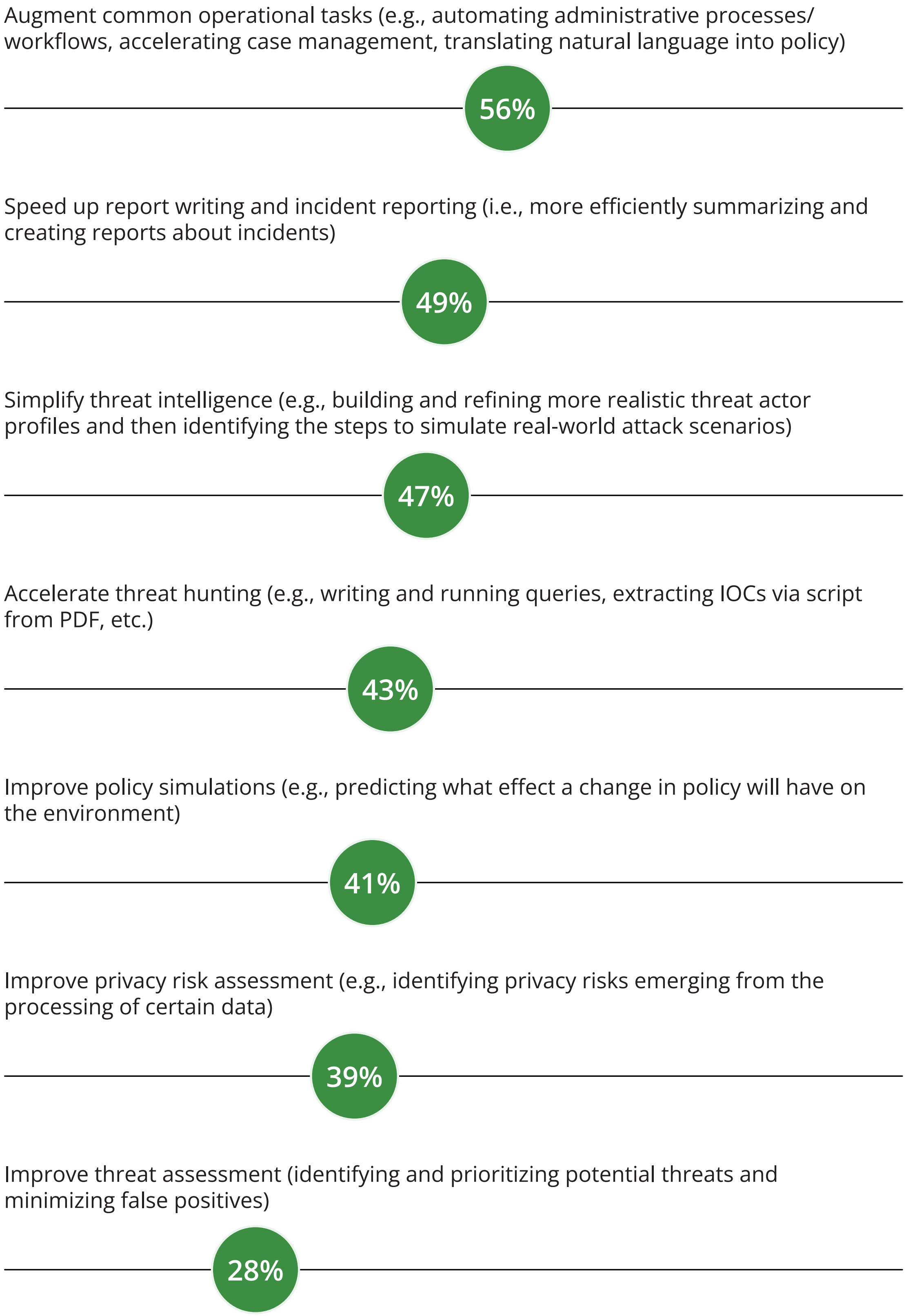
In the cybersecurity field, AI is seen as a positive force for more effectively detecting and responding to emerging threats. However, the adoption of AI across the organization (outside of cybersecurity) also increases the overall threat landscape that cybersecurity teams must protect against. Cybersecurity professionals must strike a balance between harnessing AI's potential to enhance efficiency while mitigating risks.

- **Gen AI adoption has accelerated.** 68% of respondents report Gen AI had been a significant topic of discussion by their organization's executives. Furthermore, there has been considerable momentum around Gen AI, with 64% of professionals reporting they have already implemented Gen AI at their organization. The larger the organization, the higher the rate of Gen AI usage: 73% of organizations with 20,000 or more employees have implemented Gen AI. Additionally, 45% say their organization's cybersecurity teams today have utilized Gen AI in cybersecurity tools, the top capabilities being augmenting common operational tasks, report writing and incident reporting (see Figure 18).
- **AI will benefit cybersecurity teams.** Cybersecurity teams see AI and automation as advances that will ultimately improve the workforce and their teams' ability to operate more efficiently. Professionals ranked AI and automation as the two technologies that will have the greatest impact on their ability to secure their organization (see Figure 19). But they also have concerns about advancements in AI, as they ranked it the top technology that could negatively impact organizational security. Quantum computing is also a concern, ranked second after AI and similar to last year's results.

FIGURE 18

Which of the following Gen AI capabilities do you use today within your role?

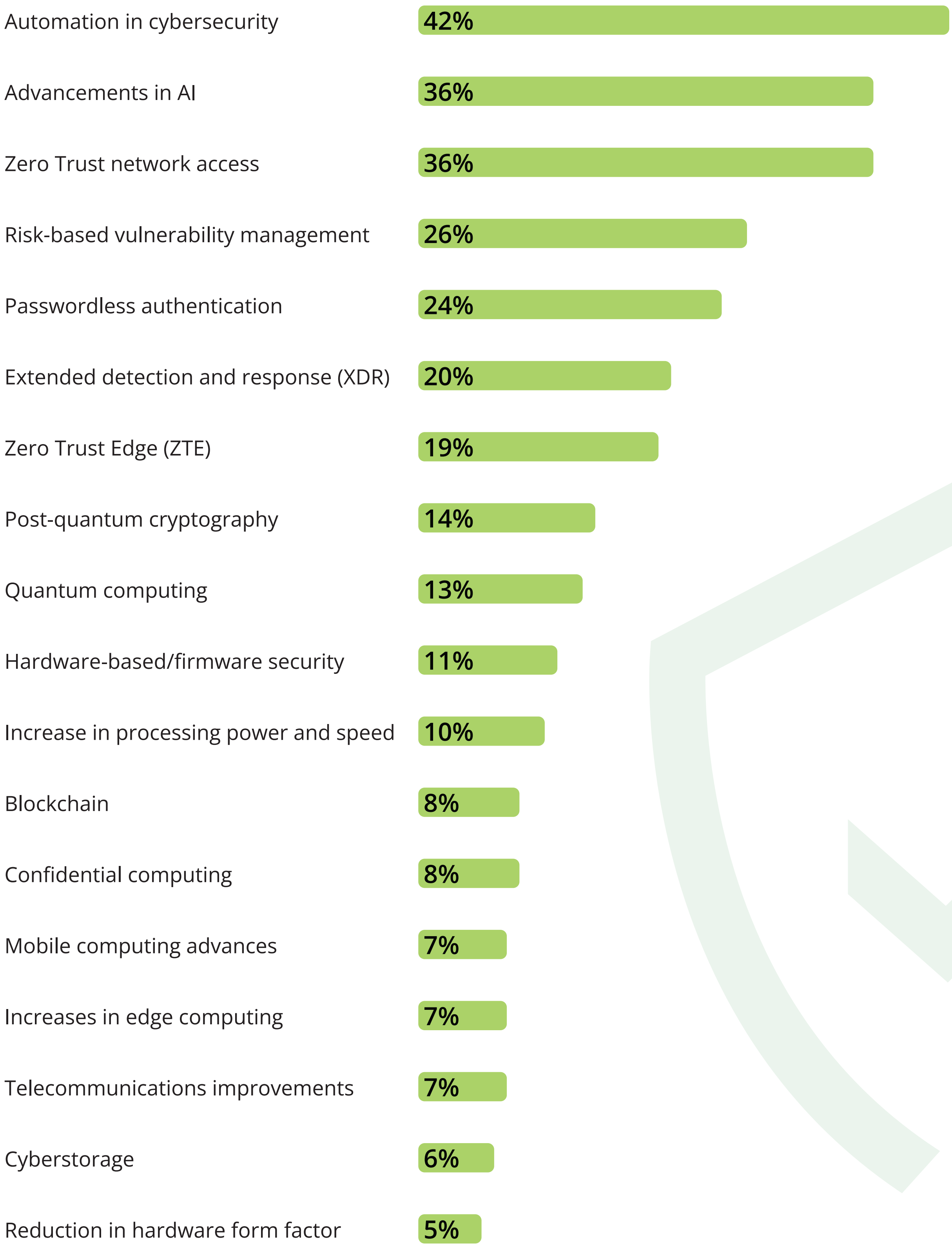
(Multiple responses accepted)



Base: 6,129 global cybersecurity professionals who use Gen AI today

FIGURE 19

Which of the following emerging cybersecurity technologies/ architectures do you believe will have the greatest positive impact on your ability to secure your organization?



Base: 15,852 global cybersecurity professionals

- **Gen AI opens the organization to new risks.** As Gen AI continues to evolve and its usage expands, the concerns associated with it become even more pronounced. Professionals already feel this, as 54% have already faced data privacy and security concerns due to organizational adoption of Gen AI. Further, increasing organizational risk is the top concern professionals have with Gen AI adoption (see Figure 20).

FIGURE 20

What are your concerns about Gen AI adoption at your organization?

53%	I worry it will open us up to greater risks
37%	I worry it won't be done strategically/methodically
32%	Gen AI has given me incorrect information in the past, and I worry it will have greater ramifications going forward
30%	I worry I can't trust its recommendations
28%	I worry that any change to accommodate Gen AI in security operations leaves us vulnerable
26%	I worry it will make my life more difficult as a cybersecurity professional
26%	I worry it's going to take significant time to adapt to new workflows
26%	I worry it won't be done ethically
12%	I worry that new workflows will slow me down compared to the way I've always done things

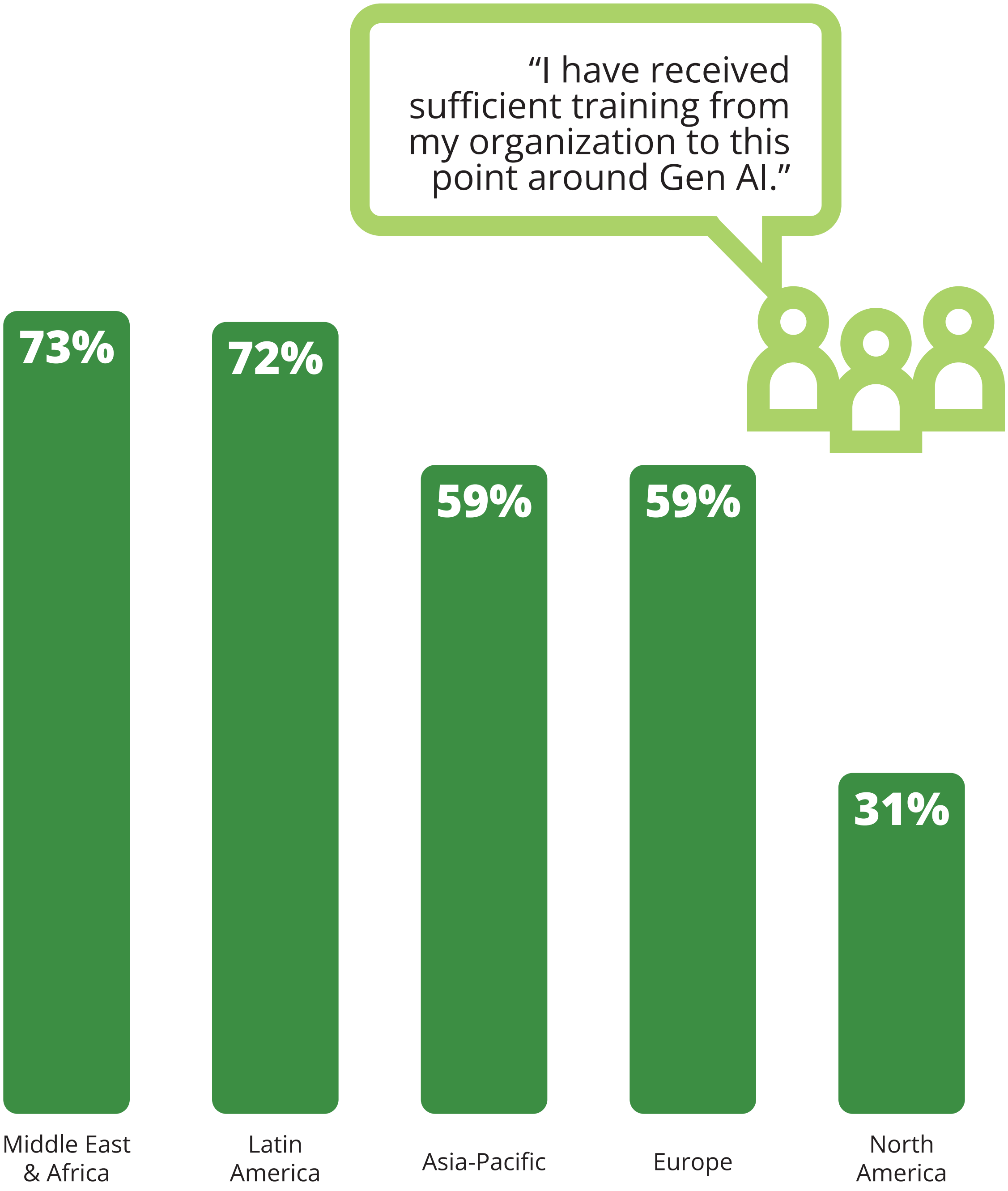
Base: 15,852 global cybersecurity professionals

This fear is not going away: 67% of professionals agree that Gen AI will pose a significant threat for cybersecurity in the future. This is especially prevalent in North America, where professionals were twice as likely to report they did not think they had received sufficient training around Gen AI (see Figure 21).

FIGURE 21

To what extent do you agree with the following statement regarding Gen AI at your organization and in cybersecurity?

(Showing "Somewhat agree/Completely agree" responses)



Base: 5,893 global cybersecurity professionals whose organizations have currently adopted Gen AI

The Way Forward

- **Organizations lack a formal strategy for Gen AI.** Lack of a clear Gen AI strategy was cited as one of the top barriers to its organizational adoption by nearly half (45%) of all participants. The C-suite and executives viewed this lack of strategy as less concerning (38% and 40%, respectively) than did directors (48%) and nonmanagerial mid- or advanced-level staff, who found it most concerning (54%).

  This lack of a clear strategy can pose challenges for organizations in effectively harnessing the potential benefits of Gen AI while mitigating associated risks, making it crucial for organizations to develop a well-defined and comprehensive strategy to guide the integration and usage of Gen AI in cybersecurity practices.

- **Guidelines will help lead the way forward.** As the adoption of Gen AI in cybersecurity continues to grow, cybersecurity professionals recognize the need for regulations and guidelines to govern its safe and responsible use. In fact, almost 90% of professionals said their organization has a Gen AI use policy. But these policies are not as advanced as they could be, as 65% of professionals say their organization needs to implement more regulations on the safe use of Gen AI.

9 out of 10
respondents said their organization has a Gen AI use policy.

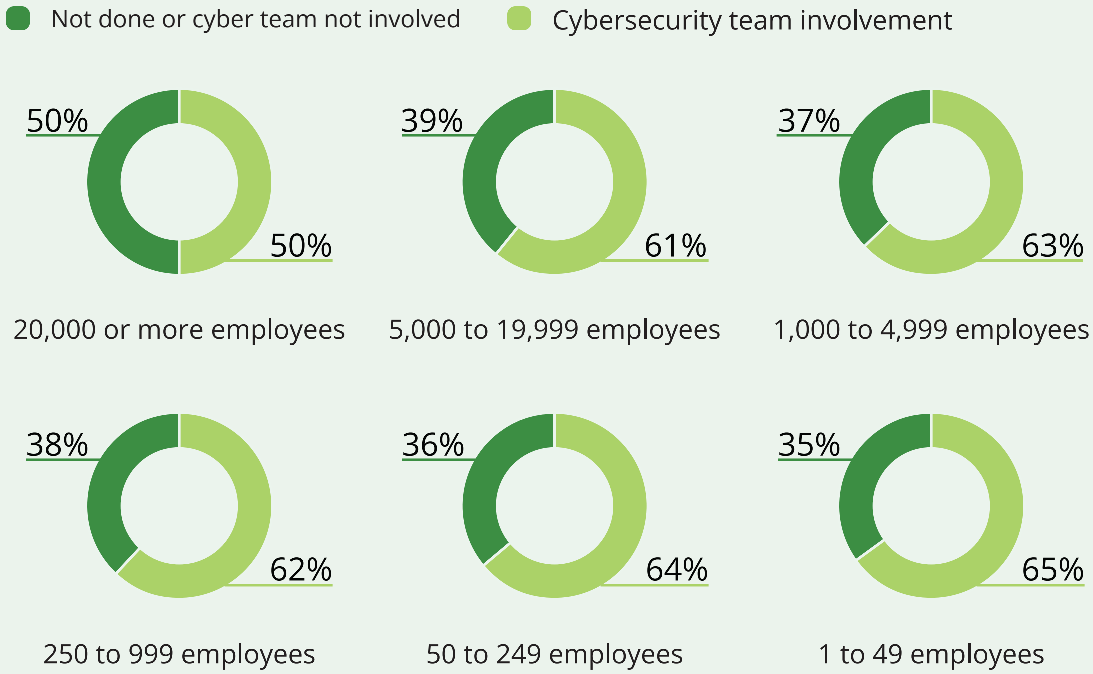
Workforce Insights

Only 60% of respondents reported that their cybersecurity team is involved with creating regulations and guidelines for Gen AI. This number is even lower for those who have 20,000 or more employees (50%) (see Figure 22).

- **Gen AI is expected to bring financial and technical benefits.** Once organizations invest in a comprehensive Gen AI strategy, the impact of the technology is predicted to be significant and far-reaching. A majority of professionals (68%) agree that within the next two years, they will be able to effectively utilize Gen AI as part of their role. They also anticipate that Gen AI will improve threat detection, improve their ability to make decisions and reduce costs for their organization. Looking ahead to the next three years, cybersecurity professionals believe that Gen AI will help reduce the impact of staffing shortages and skills gaps (see Figure 23). This highlights the immense potential of Gen AI to revolutionize the cybersecurity landscape and address critical industry challenges.

FIGURE 22

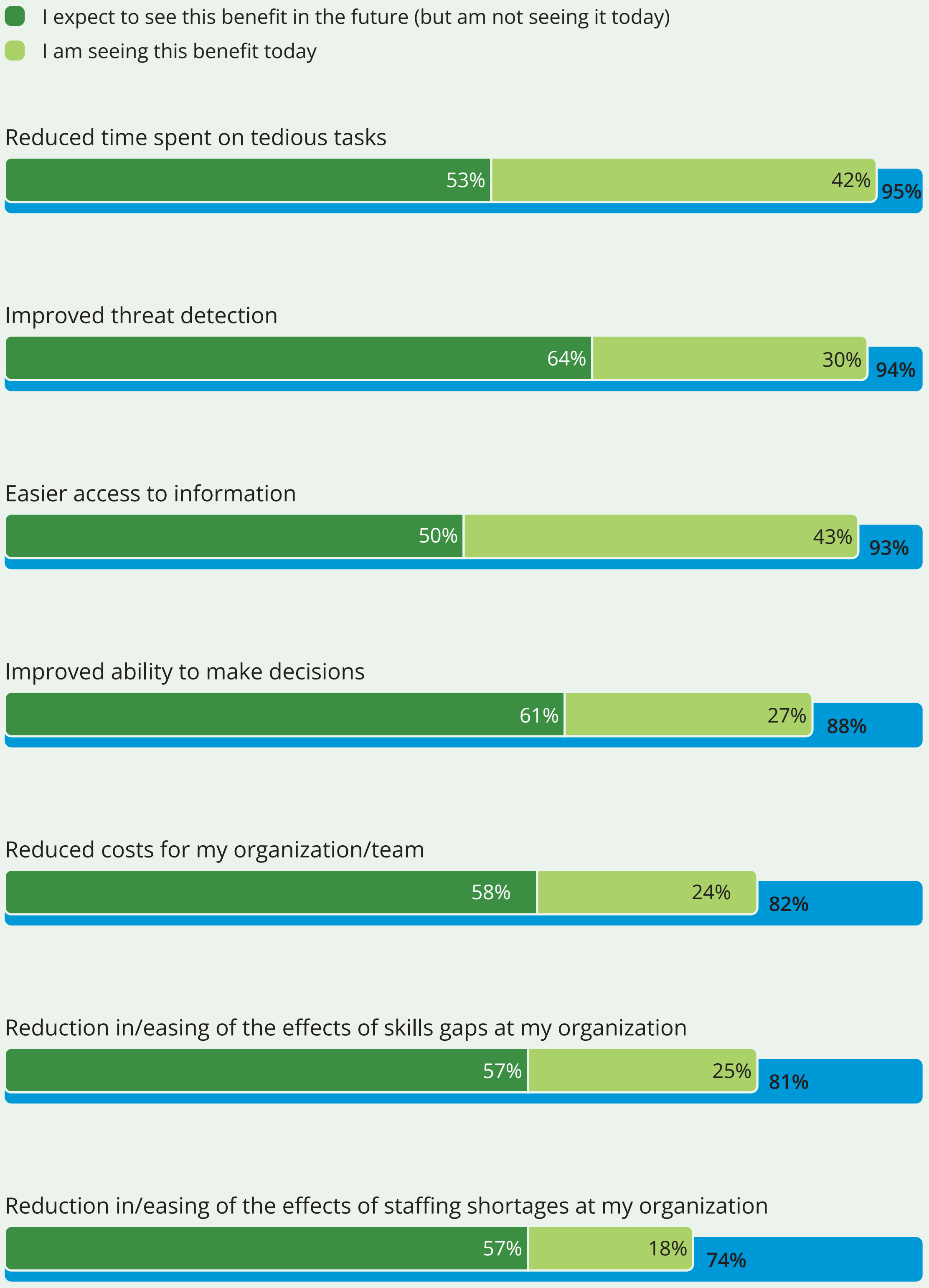
Which of the following are you or your cybersecurity team part of the decision-making process for at your organization? Creating Gen AI use policy (not specific to cybersecurity tools)?



Base: 733 -2,030 global cybersecurity professionals whose organizations have adopted Gen AI
Note: “Don’t know/does not apply” responses were removed from the sample base.

FIGURE 23

What benefits is Gen AI bringing to your organization today? What benefits do you expect it to bring in the future?



Base 5,488–14,480 global cybersecurity professionals.
Note: Individual percentage values may not sum to totals due to rounding; answer options regarding skills gaps and staff shortages were only shown to those who indicated these within their organization.

Conclusion

The 2024 ISC2 Cybersecurity Workforce Study reveals how the economy and AI are the prevailing forces redefining the environment in which cyber professionals work.

It is imperative that organizations understand and acknowledge the challenges their cybersecurity teams are facing, including staffing shortages and growing skills gaps. Organizations should not lose sight of the gains the workforce has made over the last several years. Continued growth of the global cybersecurity skills base benefits our collective security. While organizations have embraced ongoing professional development by funding training, conferences, certifications and even just providing time during working hours for staff to learn new skills, these activities cannot be viewed as luxuries for when times are good but rather as fundamental, critical elements for building and maintaining resilient cybersecurity teams.

Moreover, as businesses adopt AI as a key driver of innovation, they must consider the risks that come with it. Navigating these challenges requires more than just technical prowess — it demands careful planning; robust governance, ethical and privacy controls; and a deep understanding of evolving regulations. Cybersecurity professionals and their expertise in risk management are essential for secure AI adoption. This underscores the increasingly vital and strategic role cybersecurity professionals will play in the future of their organizations' success in an AI world.

Finally, despite the growing need for cyber professionals, global workforce growth has slowed for the first time since ISC2 began estimating the workforce size six years ago. After two years of declining investment in hiring and professional development opportunities, organizations now face significant skills and staffing shortages, and they are signaling more strongly than ever that their organizations face greater risks. Consequently, investment in skills development and enabling the next generation of the cyber workforce are more crucial than ever before, especially as we head into an AI-driven world.

Appendix

Appendix A: Demographics/Data

COMPANY SIZE	
20,000 or more	25%
10,000–19,999	7%
5,000–9,999	9%
2,500–4,999	9%
1,000–2,499	11%
500–999	9%
250–499	8%
100–249	8%
50–99	5%
20–49	3%
10–19	2%
5–9	1%
2–4	1%
1 (independent contractor or self-employed)	2%

INDUSTRY (TOP 10 SHOWN)	
IT services	21%
Financial services	11%
Government	10%
Military/military contractor	7%
Consulting	6%
Healthcare	5%
Manufacturing	4%
Telecommunications	4%
Security software/ hardware development	3%
Education	3%

RESPONDENT LEVEL	
C-level executive	5%
Executive management	5%
Director/middle manager	20%
Manager	21%
Nonmanagerial mid- or advanced-level staff	40%
Entry-/junior-level staff	3%
Independent contractor/ consultant	4%
Other	1%

ROLE (TOP 10 SHOWN)	
Security engineer	7%
IT security manager	7%
Security consultant/advisor	6%
IT manager	6%
IT director	5%
IT security director	5%
Security architect	5%
Security analyst	4%
CISO	4%
Security specialist	3%

INTERNAL/EXTERNAL	
Internal security staff for my organization	62%
Security consultant or consultancy	14%
External security service provider (e.g., MSSP, external SOC, independent contractor, etc.)	12%
Other	6%

TIME SPENT ON SECURITY	
100% of a typical week	19%
75%–99%	23%
50%–74%	24%
25%–49%	20%
1%–24%	13%
0%	1%

FOCUS OF CYBERSECURITY ROLE	
Cybersecurity governance and risk management	16%
Cybersecurity management	14%
Cybersecurity generalist	12%
Secure system architecture and design	10%
Secure operations	7%
Cybersecurity audit and assurance	6%
Data protection and privacy	5%
Secure system development	4%
Network monitoring and intrusion detection	4%
Identity and access management	4%
Cyberthreat intelligence	3%
Vulnerability management	3%
Incident response	3%
Security testing	2%
Cryptography and communications security	2%
Digital forensics	1%
Other	3%

HIRING AUTHORITY	
Yes, I make final decisions about hiring	23%
Yes, I am part of a team that makes hiring decisions	26%
I interview candidates and influence decisions but do not make final decisions	26%
I do not have hiring authority or influence over decisions about hiring	25%

GENDER	
Female	14.4%
Male	79.6%
Intersex	0.1%
Transgender	0.2%
Nonbinary	0.3%
Prefer to self-describe	0.1%
Prefer not to say	5.5%

AGE	
23 or younger	0.1%
23–29	4.7%
30–34	11.4%
35–38	12.9%
39–44	21.9%
45–49	16.0%
50–54	12.6%
55–59	8.4%
60–64	5.1%
65–73	2.0%
74 or older	0.1%
Prefer not to say	4.6%

NEURODIVERGENCE SELF-REPORTING	
Yes	13%
No	75%
Prefer not to answer	6%
Don’t know	7%

COUNTRY	
United States	46%
Japan	6%
United Kingdom	6%
Canada	4%
China	4%
Germany	3%
Singapore	3%
Australia	3%
Netherlands	3%
India	3%
France	2%
Spain	2%
South Korea	2%
Brazil	1%
Republic of Ireland	1%
United Arab Emirates	1%
Mexico	1%
South Africa	1%
Saudi Arabia	1%
Nigeria	1%
Taiwan	1%
Hong Kong	1%
Switzerland	1%
Other	6%

US STATE (TOP 10 SHOWN)	
Virginia	9%
California	9%
Texas	8%
Florida	6%
Maryland	6%
Colorado	4%
Georgia	3%
Pennsylvania	3%
New York	3%
Illinois	3%

Appendix B: Workforce Estimate and Gap Methodology

WORKFORCE ESTIMATE METHODOLOGY

The estimate of the global cybersecurity workforce begins with estimates of the US workforce, as the US provides a crucial combination of a robust sample and reliable secondary data sources. The US estimate is derived from three main methodological groups:

1. **Survey-based Estimates.** Survey data on the number of cybersecurity professionals who are employed by organizations is combined with secondary data estimating the number of US business entities in various size strata. These secondary sources include: the US Bureau of Labor Statistics' Quarterly Census of Employment and Wages; the US Census's Statistics of US Businesses Survey; and the US Census's County Business Patterns study.

2. **Third-party Estimates.** Various estimates of related populations were modified based on survey findings to match our estimation criteria. This includes the US Bureau of Labor Statistics' estimate of cybersecurity analysts.

3. **Trending Estimates.** Previous years' estimates were trended using multiple methodologies to provide expected estimates for this year's numbers.

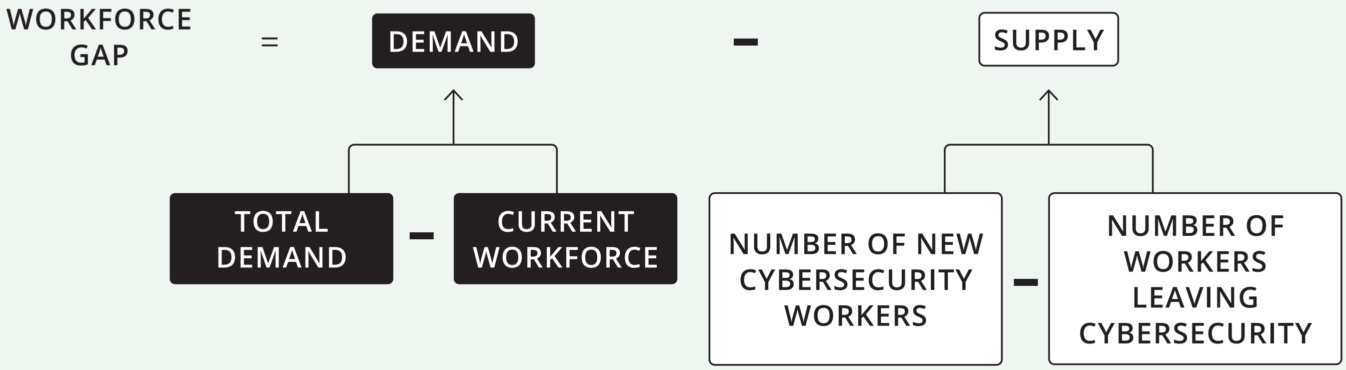
The US estimate provides a baseline for the estimates of the rest of the world. Estimates for other countries used similar methods but replaced third-party estimates with estimates derived from the US baseline; most countries did not have reliable third-party estimates. The secondary data estimates for countries outside of the US came primarily from the Organisation for Economic Co-operation and Development (OECD). China and India, while included in the gap estimate, were excluded from the workforce estimate due to a lack of reliable secondary sources.

GAP ESTIMATE METHODOLOGY

The workforce gap used similar approaches to the estimate of the total cybersecurity workforce. A combination of survey-based, trending and third-party methodologies provided the US estimate, which was then used as the baseline for the rest of the world. The basic calculation for the workforce gap comes down to gap = demand - supply.

- Demand is defined as the number of cybersecurity jobs organizations would like to employ over the next year, minus the number of current workers.
- Supply is defined as the number of workers who will enter the field over the next 12 months, minus the number of workers who will leave the field.

In total, this makes the equation for calculating the gap: workforce gap = (total demand over the next 12 months - the current workforce) - (number of workers entering the field - number of workers leaving the field).


WORKFORCE GAP
=
DEMAND
-
SUPPLY
TOTAL DEMAND
-
CURRENT WORKFORCE
NUMBER OF NEW CYBERSECURITY WORKERS
-
NUMBER OF WORKERS LEAVING CYBERSECURITY

The workforce gap calculates the difference between the number of cybersecurity professionals organizations require to properly secure themselves and the number of cybersecurity professionals available for hire. The workforce gap does not aim to estimate the actual current job market for cybersecurity professionals. During times of economic uncertainty, many organizations have made cutbacks involving hiring freezes and layoffs, which we discuss in more detail throughout this study. This, however, does not affect the workforce gap because organizations' need for cybersecurity workers remains the same, regardless of whether or not those organizations currently have the funds to actually hire and employ sufficient staff.

Appendix C: Supplemental Material

ABOUT ISC2

ISC2 is the world's leading member organization for cybersecurity professionals, driven by our vision of a safe and secure cyber world. Our nearly 675,000 members, candidates and associates around the globe are a force for good, safeguarding the way we live. Our award-winning certifications — including cybersecurity's premier certification, the CISSP® — enable professionals to demonstrate their knowledge, skills and abilities at every stage of their careers. ISC2 strengthens the influence, diversity and vitality of the cybersecurity profession through advocacy, expertise and workforce empowerment that accelerates cyber safety and security in an interconnected world. Our charitable foundation, The Center for Cyber Safety and Education, helps create more access to cyber careers and educate those most vulnerable. Learn more and get involved at ISC2.org. Connect with us on X, Facebook and LinkedIn.

ABOUT THE ISC2 CYBERSECURITY WORKFORCE STUDY

ISC2 conducts in-depth research into the challenges and opportunities facing the cybersecurity profession. The ISC2 Cybersecurity Workforce Study is conducted annually to assess the cybersecurity workforce gap; better understand the barriers facing the cybersecurity profession; and uncover solutions that enable individuals to excel in their profession, achieve their career goals and better secure their organizations' critical assets.

The 2024 ISC2 Cybersecurity Workforce Study is based on online survey data collected in collaboration with Forrester Research, Inc. in April and May 2024 from 15,852 individuals responsible for cybersecurity at workplaces throughout North America; Latin America (LATAM); the Asia-Pacific region (APAC); and Europe, the Middle East and Africa (EMEA). Respondents in non-English-speaking countries completed a locally translated version of the survey.

Learn more at www.isc2.org/research.

ISC2™