ISC2 CYBERSECURITY WORKFORCE STUDY

ISC2™

How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce

2023

Table of Contents

Executive Summary

Cybersecurity professionals are facing greater pressures than ever that diminish their ability to defend institutions and organizations around the world from ever-increasing threats.

Dealing with emerging challenges with grave consequences is not a new phenomenon for cybersecurity professionals. However, our study shows that a perfect storm of economic uncertainty, rapidly emerging technologies, fragmented regulations and ever-widening workforce and skills gaps is creating huge uncertainty for a profession whose role it is to protect global infrastructure and systems from attack. The cybersecurity workforce needs more support and investment from leaders across the public and private sectors.

This piles on top of nearly three years of rapidly evolving business and threat environments that started with cybersecurity professionals securely transitioning their organizations through accelerated work-from-home and cloud services deployments in response to the COVID-19 pandemic. And critical vulnerabilities across entrenched platforms continue to be exploited throughout the IT services and software supply chains. When war broke out in Eastern Europe, the conflict in Ukraine ushered in a new era of cyber warfare.

Today, cybersecurity professionals continue to contend with challenges that have built since the outbreak of COVID, while also facing the consequences of greater economic pressure across the globe. Cybersecurity leaders and professionals at all levels are adjusting to staff layoffs and budget cutbacks. For the first time since the beginning of the 2020 pandemic, many study participants expect cybersecurity hiring to decrease in their organizations over the next year. The pressure on the workforce is real, with our study finding a modest decrease in job satisfaction for the first time. Many professionals remain concerned that leadership in their organizations does not listen to their guidance, which creates additional risk. They also say the threat landscape is the worst it's been in the last five years, with reports of malicious insiders increasing.

Meanwhile, the disruptive arrival of the latest generation of artificial intelligence brings additional uncertainty. Will AI advance how we identify and respond to threats? Will AI force us to rethink security roles and responsibilities that may eliminate jobs or create new ones? Does AI herald a new era of rapidly evolving threats? Will AI foster a combination of all three scenarios, as well as others we have not yet imagined? Cybersecurity professionals remain both optimistic and cautious about AI.

Despite these headwinds, the workforce — and demand for their expertise — continues to grow. We estimate the size of the global cybersecurity workforce at 5.5 million — a 9% increase from 2022, and the highest we've ever recorded. Conversely, the global workforce gap continues to grow even faster: The gap grew by 13% from 2022, which means that in 2023 there are roughly 4 million cybersecurity professionals needed worldwide. The profession needs to almost double to be at full capacity.

Our study also reveals how the ongoing workforce gap and pressures from budget cutbacks and layoffs are creating critical workforce skills gaps. Study participants expressed concern that skills gaps leave their organizations more vulnerable than the lack of qualified team members. This is highlighted even more as rapidly evolving technologies like AI expose gaps in knowledge and experience, as well as in risk management processes. Organizations and policymakers need strategies to address both, and our study reveals solutions to help mitigate these risks despite the global workforce and skills deficits.

75%

said the current threat landscape is the most challenging it has been in the past five years.

Our review of career pathways, shifting demographics for new entrants into the field, adoption of new hiring practices and investment in developing and retaining existing staff reveal how organizations are mitigating risk, keeping staff engaged and offsetting the impacts of budget cutbacks.

For this report, we surveyed a larger and more geographically diverse audience than ever before — 14,865 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. We are pleased to celebrate and share their creativity, resiliency and dedication. This report presents valuable findings to cybersecurity professionals and leaders, executives, policymakers and others to reveal solutions to the top challenges facing the workforce today.

Key Findings

THE CYBERSECURITY WORKFORCE AND GAP HAVE BOTH GROWN. In the past year, the cybersecurity workforce has grown by 8.7%. In addition, the gap between the number of workers needed and the number available has also continued to grow, with a 12.6% increase year over year.

CYBERSECURITY HAS NOT BEEN IMMUNE TO CUTBACKS. 47% of cybersecurity professionals have dealt with cutbacks to their teams in the form of layoffs, budget cuts and hiring or promotion freezes. 22% have experienced layoffs, and 31% expect additional cutbacks in the next year.

STAFFING SHORTAGES AND SKILLS GAPS ARE CONSISTENT CHALLENGES. 67% of respondents reported that their organization has a shortage of cybersecurity staff needed to prevent and troubleshoot security issues. And 92% report having skills gaps in their organization — the most common being cloud computing security, AI/ML and Zero Trust implementation. We will examine these skills gaps in depth this year as 67% of those whose organizations had both shortages in total staff and skills gaps say that skills gaps are often worse.

ONGOING EDUCATION AND TRAINING HELP SHRINK SKILLS GAPS. 58% of cybersecurity professionals said that the negative impact of worker shortages can be mitigated by filling key skills gaps. We found that those who continue their training, education and certification reimbursement programs were far better prepared to weather times of economic uncertainty. Organizations with layoffs who kept these programs, were less likely to experience significant organizational skills gaps in cybersecurity.

CYBERSECURITY PROFESSIONALS FACE AN UNPRECEDENTED THREAT LANDSCAPE. 75% of cybersecurity professionals view the current threat landscape as the most challenging it has been in the past five years, and only 52% believe that their organization has the tools and people needed to respond to cyber incidents over the next two to three years. Those with shortages and skills gaps are far more worried about being able to keep their organizations secure.

TIMES OF ECONOMIC UNCERTAINTY POSE SIGNIFICANT THREATS TO CYBERSECURITY. 71% of respondents agree that periods of economic uncertainty increase the risk of malicious insiders. Our study found that 39% of cybersecurity professionals have been approached or know someone who has been approached by a malicious actor. Those at companies that have had layoffs in cybersecurity are three times more likely to have been approached to act as a malicious insider.

JOB SATISFACTION TOOK A SLIGHT DIP BUT REMAINS HIGH. 70% of cybersecurity professionals say they are satisfied with their jobs today, which represents a 4% drop from last year. This seems to be due in large part to cutbacks and layoffs, which our study shows significantly impact job satisfaction through overwork and loss of employee trust.

PATHWAYS INTO CYBERSECURITY ARE SHIFTING. We saw a significant shift in who is entering the cybersecurity profession and how they are doing it. Our study found that new workers are significantly more likely to have received a bachelor's degree in cybersecurity before entering the field and are also more likely to previously have worked in a non-IT role. They are less likely to have worked in IT before entering. We also found that there are significantly more people entering cybersecurity later in their career and that the gender and ethnic breakdowns of the new workforce have undergone a considerable shift.

ORGANIZATIONS NEED PROFESSIONALS WITH CLOUD COMPUTING SKILLS, BUT THEY ARE HARD TO FIND. Our study found that cloud computing security is the skill that hiring managers most look for when hiring. However, it is also the most common area where respondents cited their organization having a skills gap.

AI/ML IS BECOMING INCREASINGLY CRITICAL. This year, for the first time, AI/ML skills were among the top five in terms of demand, representing a significant jump since last year when they were near the bottom of the list.

CYBERSECURITY PROFESSIONALS VALUE EXPERIENCE OVER FORMAL EDUCATION. We asked cybersecurity professionals to compare qualifications to understand what they value most in potential candidates and found that they value experience over education. Professionals favor senior-level experience over doctorate degrees (86% vs. 14%) and entry-level cybersecurity experience over cybersecurity bachelor's degrees (70% vs. 30%).

Workforce Gap & Estimate

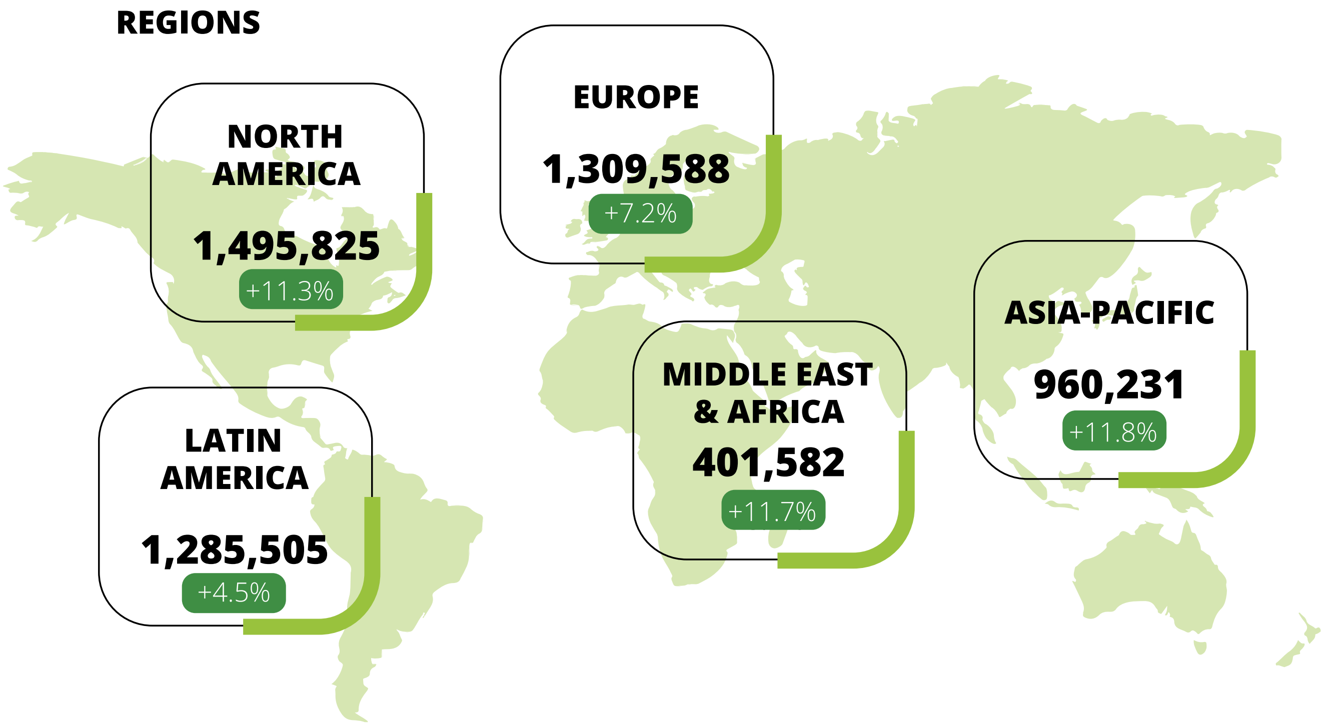
Cybersecurity is evolving, and so is its workforce. To better understand this ever-changing field, we first need to understand its scope and scale — how it is growing and whether the supply of new workers is keeping up with organizational demand. In order to achieve this, ISC2 introduced the cybersecurity workforce estimate in 2019. This proprietary methodology integrates 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). This year, this number includes four new countries not previously included in ISC2's global estimate: Saudi Arabia, the United Arab Emirates, Nigeria and South Africa.

ISC2 estimates the global cybersecurity workforce at 5.5 million, representing an 8.7% increase year over year and nearly 440,000 new jobs. All regions saw growth this year, but these gains are particularly high in our two new Middle East countries, Asia-Pacific and North America. Japan in particular is growing at a rapid rate — 24% year over year. Latin America, after years of substantial growth, is starting to balance out, with Brazil decreasing from an 18.3% growth rate in 2022 to 8.9% this year, and Mexico dropping slightly year over year (see figures 1-A and 1-B).

FIGURE 1-A

2023 Global Cybersecurity Workforce

5,452,732 +8.7% YoY*

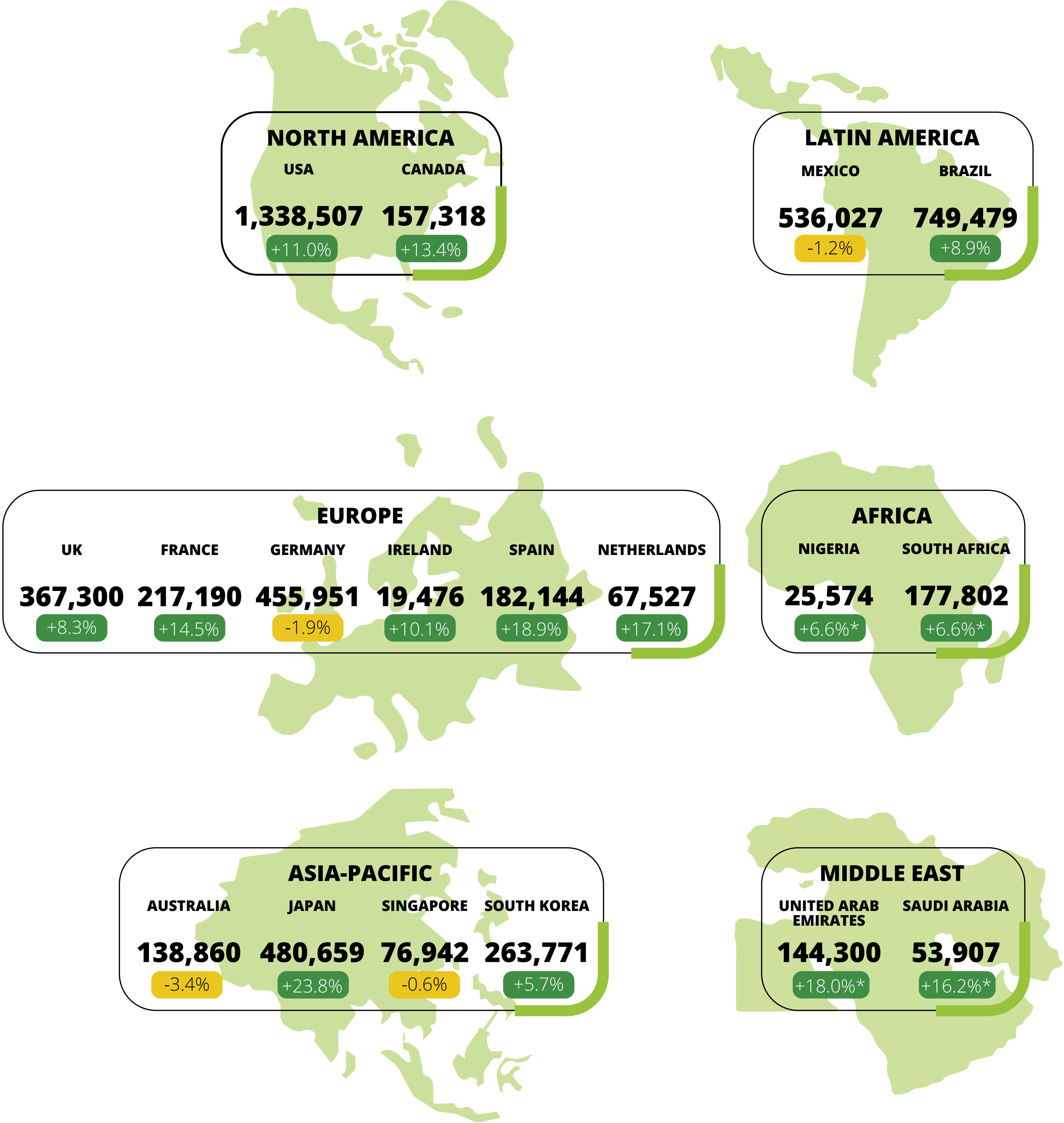


*2023 estimate includes four new countries — United Arab Emirates, Saudi Arabia, Nigeria and South Africa. YoY growth is based on back-estimates for those countries for 2022.

FIGURE 1-B

2023 Global Cybersecurity Workforce Estimate

5,452,732 +8.7% YoY*



NORTH AMERICA

USA	CANADA
1,338,507	157,318
+11.0%	+13.4%

LATIN AMERICA

MEXICO	BRAZIL
536,027	749,479
-1.2%	+8.9%

EUROPE

UK	FRANCE	GERMANY	IRELAND	SPAIN	NETHERLANDS
367,300	217,190	455,951	19,476	182,144	67,527
+8.3%	+14.5%	-1.9%	+10.1%	+18.9%	+17.1%

AFRICA

NIGERIA	SOUTH AFRICA
25,574	177,802
+6.6%*	+6.6%*

ASIA-PACIFIC

AUSTRALIA	JAPAN	SINGAPORE	SOUTH KOREA
138,860	480,659	76,942	263,771
-3.4%	+23.8%	-0.6%	+5.7%

MIDDLE EAST

UNITED ARAB EMIRATES	SAUDI ARABIA
144,300	53,907
+18.0%*	+16.2%*

*2023 estimate includes four new countries — United Arab Emirates, Saudi Arabia, Nigeria and South Africa. YoY growth is based on back-estimates for those countries for 2022.

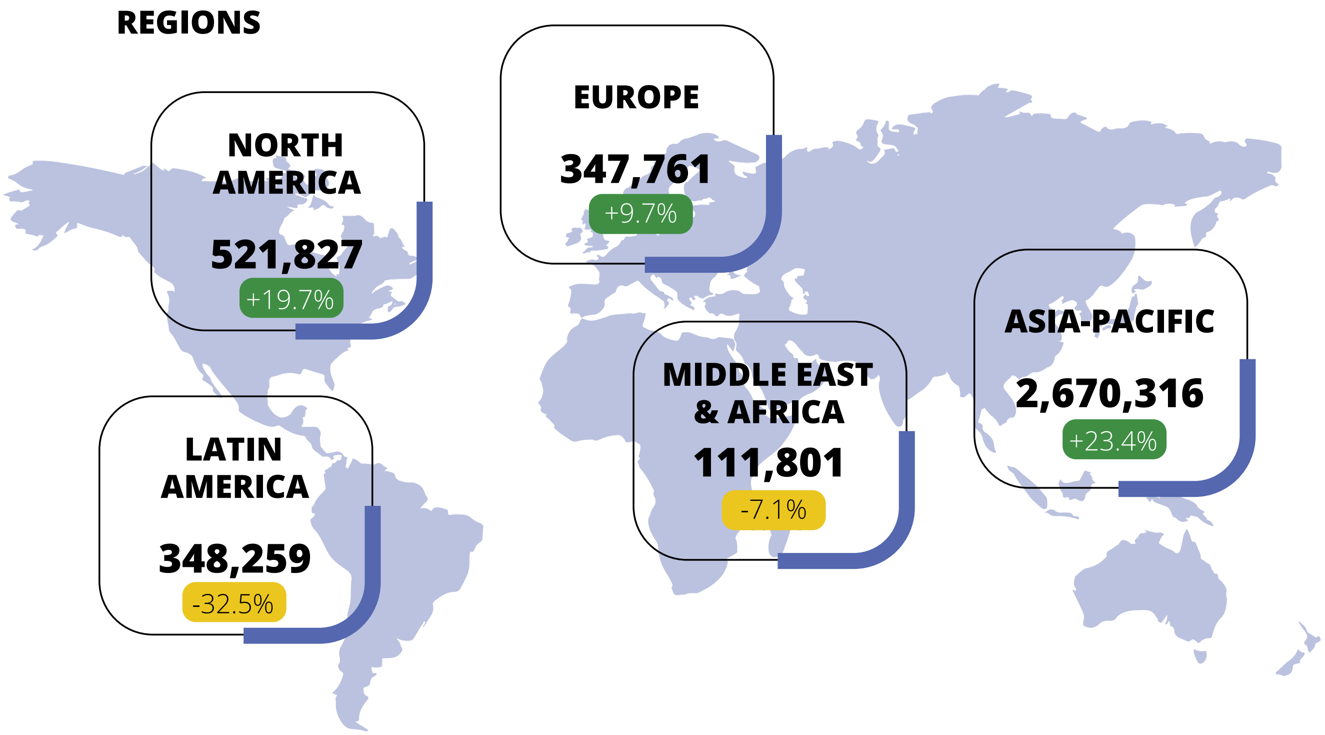
Despite the continued growth in the workforce, ISC2's cybersecurity workforce study revealed that demand is still outpacing supply. The workforce gap grew an additional 12.6% this year, with the greatest rise in Asia-Pacific (especially Japan and India) and North America. Areas with particularly rapid growth in supply like the Middle East and Latin America are starting to finally see demand catch up such that the workforce gap actually shrank this year (see figures 2-A and 2-B).

It's important to note what this year's workforce gap represents. The workforce gap calculates the difference between the number of cybersecurity professionals that 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 paper. 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.

FIGURE 2-A

2023 Global Cybersecurity Workforce Gap

3,999,964 +12.6% YoY*

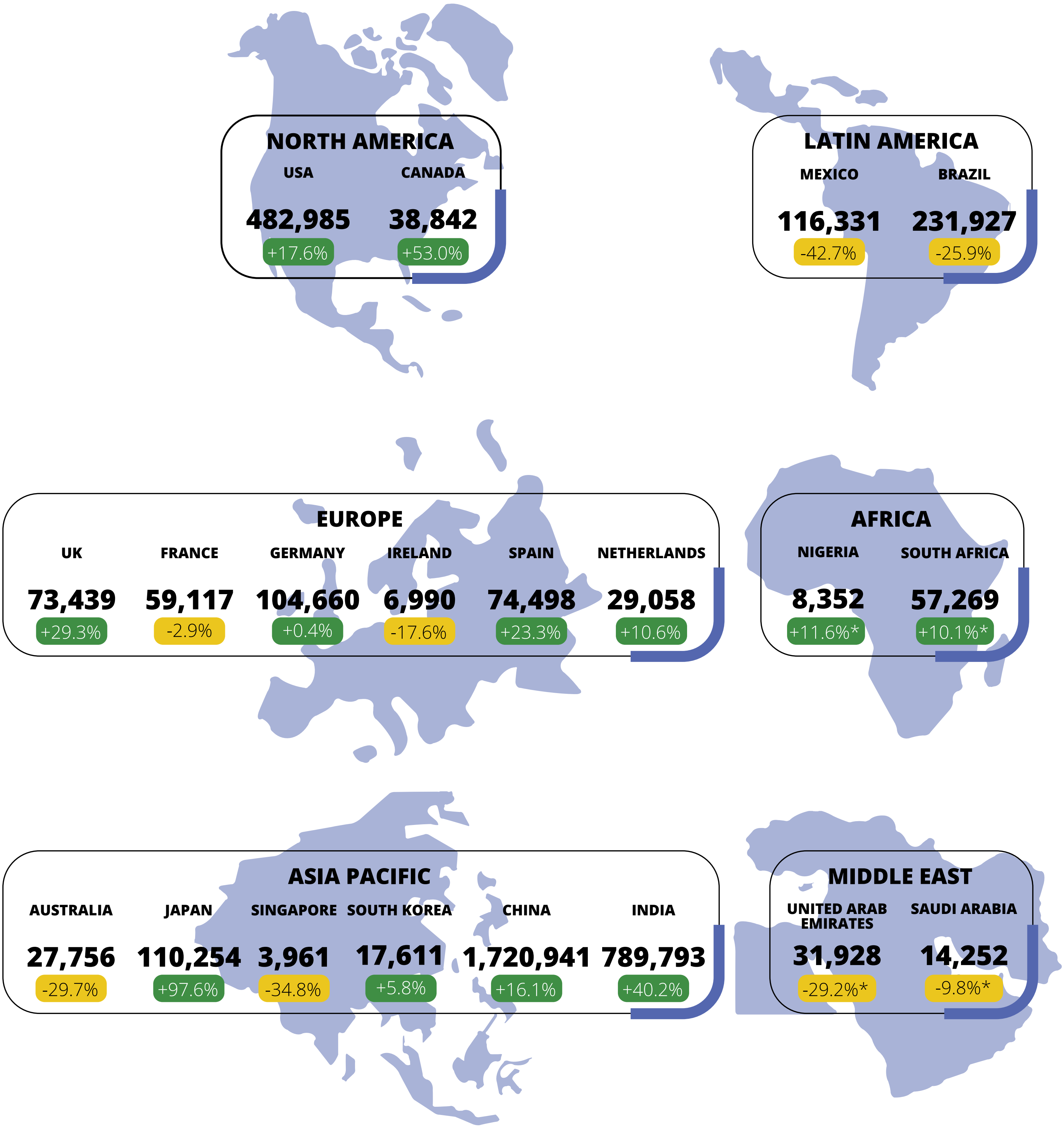


*2023 gap includes 4 new countries – United Arab Emirates, Saudi Arabia, Nigeria and South Africa. YoY growth are based on back estimates for those countries for 2022

FIGURE 2-B

2023 Global Cybersecurity Workforce Gap

3,999,964 +12.6% YoY*



NORTH AMERICA

USA	CANADA
482,985	38,842
+17.6%	+53.0%

LATIN AMERICA

MEXICO	BRAZIL
116,331	231,927
-42.7%	-25.9%

EUROPE

UK	FRANCE	GERMANY	IRELAND	SPAIN	NETHERLANDS
73,439	59,117	104,660	6,990	74,498	29,058
+29.3%	-2.9%	+0.4%	-17.6%	+23.3%	+10.6%

AFRICA

NIGERIA	SOUTH AFRICA
8,352	57,269
+11.6%*	+10.1%*

ASIA PACIFIC

AUSTRALIA	JAPAN	SINGAPORE	SOUTH KOREA	CHINA	INDIA
27,756	110,254	3,961	17,611	1,720,941	789,793
-29.7%	+97.6%	-34.8%	+5.8%	+16.1%	+40.2%

MIDDLE EAST

UNITED ARAB EMIRATES	SAUDI ARABIA
31,928	14,252
-29.2%*	-9.8%*

*2023 estimate includes four new countries — United Arab Emirates, Saudi Arabia, Nigeria and South Africa. YoY growth is based on back-estimates for those countries for 2022.

Current State of the Cybersecurity Workforce

Cutbacks and economic uncertainty add to the existing skills gap challenge

The current macroeconomic environment has normalized higher costs, lower revenue and worker shortages. As a result, many organizations are choosing to implement cost-saving cutbacks (e.g., budget cuts, layoffs, hiring freezes and promotion freezes) to support their balance sheet. However, these organizational cutbacks — especially within cybersecurity teams — have implications that extend beyond just cost.

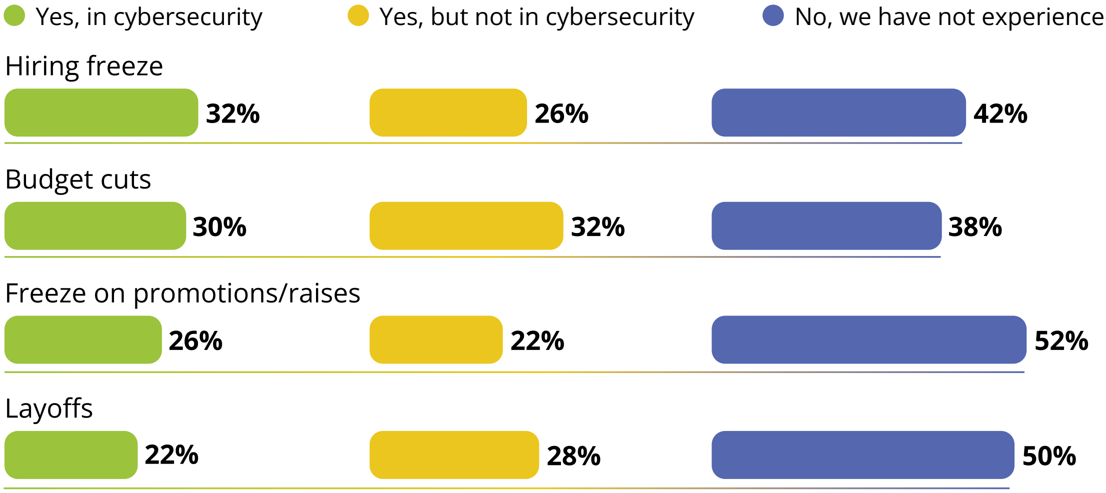
Cybersecurity professionals are critical protectors against risk and vulnerability, but cutbacks throttle their productivity, satisfaction and skill development. In this study, cybersecurity professionals share how cutbacks and related challenges like staffing shortages and skills gaps truly impact their day-to-day work, so organizations can discover opportunities for improvement.

After surveying 14,865 cybersecurity professionals, we found that:

- **Cutbacks are a pervasive challenge for cybersecurity professionals**. Overall, 47% of cybersecurity workers have experienced cybersecurity-related cutbacks (layoffs, budget cuts, hiring or promotion freezes) — and 22% of this group have been impacted by layoffs (both firsthand and secondhand) within cybersecurity. An additional 28% have had layoffs elsewhere in their organizations, which can significantly affect the cybersecurity workforce (see figure 3). 41% of respondents feel as though cutbacks have affected their security team disproportionately in comparison to the rest of their organization. And, as we'll discuss more in depth later in the paper, cutbacks to both the cybersecurity team and the rest of the organization can create significant cybersecurity risks.

FIGURE 3

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



Base: 11,656-12,200 global cybersecurity professionals
Note: "Don't know/does not apply" responses were removed from the sample base.

- **Cutbacks impact some industries and regions significantly more than others.** All major industries have experienced cutbacks, but the entertainment, construction, automotive and tech sectors have been hit particularly hard by layoffs in cybersecurity (see figure 4). Geographically, Latin America has seen the greatest layoffs, followed by the Middle East and Africa (see figure 5). Latin America has seen rapid growth over the past few years within its cybersecurity workforce, so this could be the beginning of a level-setting for that growth as the workforce more accurately reflects demand.

FIGURE 4

Has your organization experienced layoffs in the past 12 months?

(Showing percentage of layoffs in cybersecurity in the past year)

INDUSTRIES WITH FEWEST LAYOFFS IN CYBER	
Military/military contractor	8%
Government (non-military)	9%
Education	13%
Aerospace	13%
Transportation	16%

INDUSTRIES WITH MOST LAYOFFS IN CYBER	
Entertainment/media	33%
Construction	31%
Security software/ hardware development	31%
Automotive	29%
Hosted/cloud services	29%

Base: 145-1,306 global cybersecurity professionals in listed industries
Note: "Don't know/does not apply" responses were removed from the sample base.

FIGURE 5

Has your organization experienced layoffs in the past 12 months?

(Showing percentage of layoffs in cybersecurity in the past year)

COUNTRIES WITH FEWEST LAYOFFS IN CYBER	
Hong Kong	11%
United States	18%
Saudi Arabia	19%
Canada	21%
Singapore	23%

COUNTRIES WITH MOST LAYOFFS IN CYBER	
Brazil	38%
Mexico	37%
Nigeria	33%
United Arab Emirates	33%
China	31%

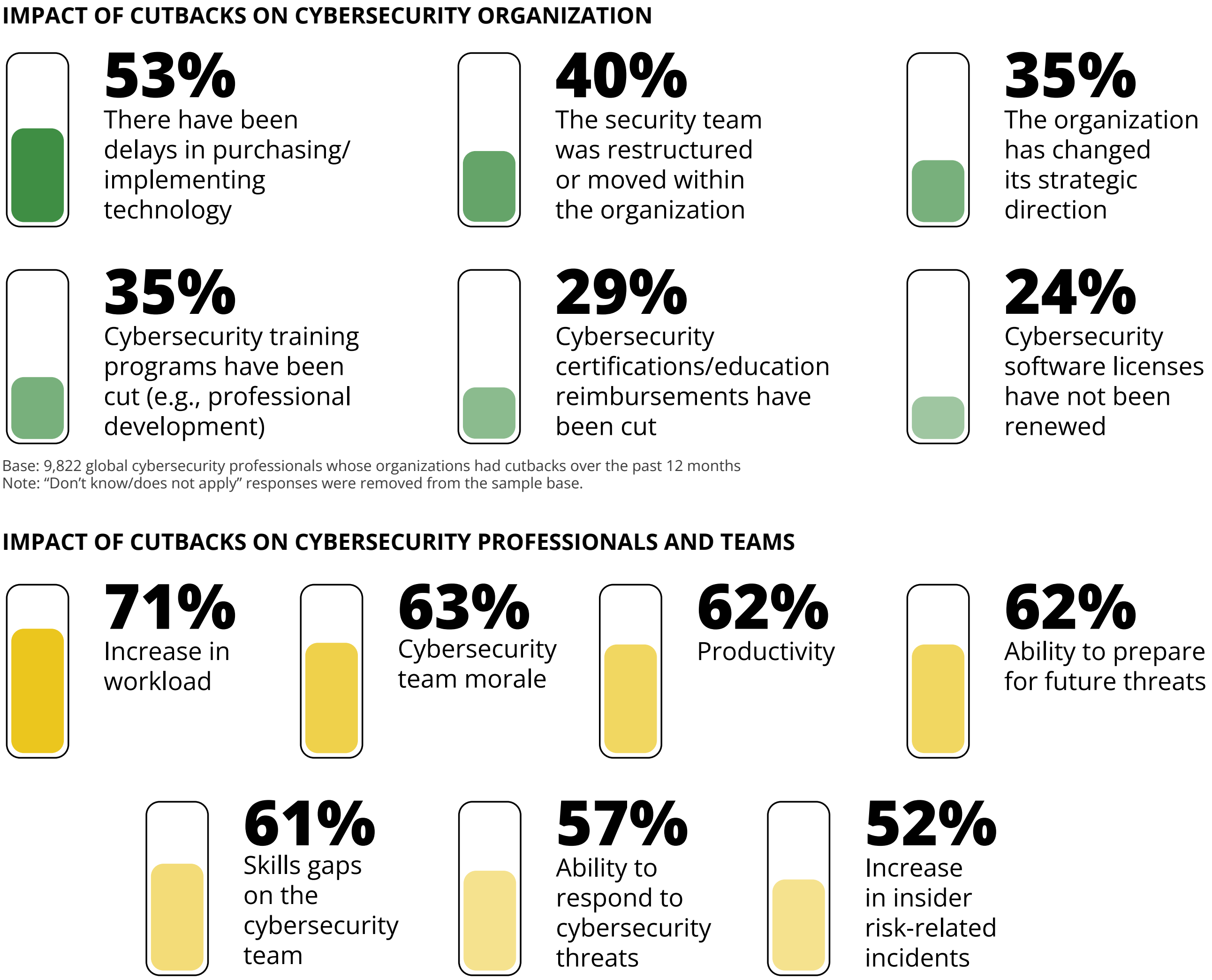
Base: 121-5,479 global cybersecurity professionals in listed countries
Note: "Don't know/does not apply" responses were removed from the sample base.

- **Cutbacks create a ripple effect for cybersecurity teams.** As a result of cutbacks, organizations are consolidating resources and restructuring, often changing the way cybersecurity professionals operate. 53% say that cutbacks have resulted in delays in purchasing or implementing technology, while 40% of those with cutbacks have had their security teams restructured or moved within their organization. 35% have even eliminated cybersecurity training programs, which are a critical resource for developing skills and closing skills gaps.

  Cutbacks also impact cybersecurity organizations at the team and individual level. 71% of cybersecurity professionals have experienced a negative impact on their workload as a result of cutbacks. Almost two-thirds of professionals say that cutbacks also degrade productivity, team morale and the ability to prepare for future threats. Insider risk and threat response are two additional key elements of the impact of cutbacks at the team level. More than half of professionals (57%) felt that their threat response was inhibited by organizational cutbacks, and 52% saw an increase in insider risk-related incidents (see figure 6).

FIGURE 6

Which of the following effects has your organization/team experienced as a result of cutbacks?



Base: 9,822 global cybersecurity professionals whose organizations had cutbacks over the past 12 months
Note: "Don't know/does not apply" responses were removed from the sample base.

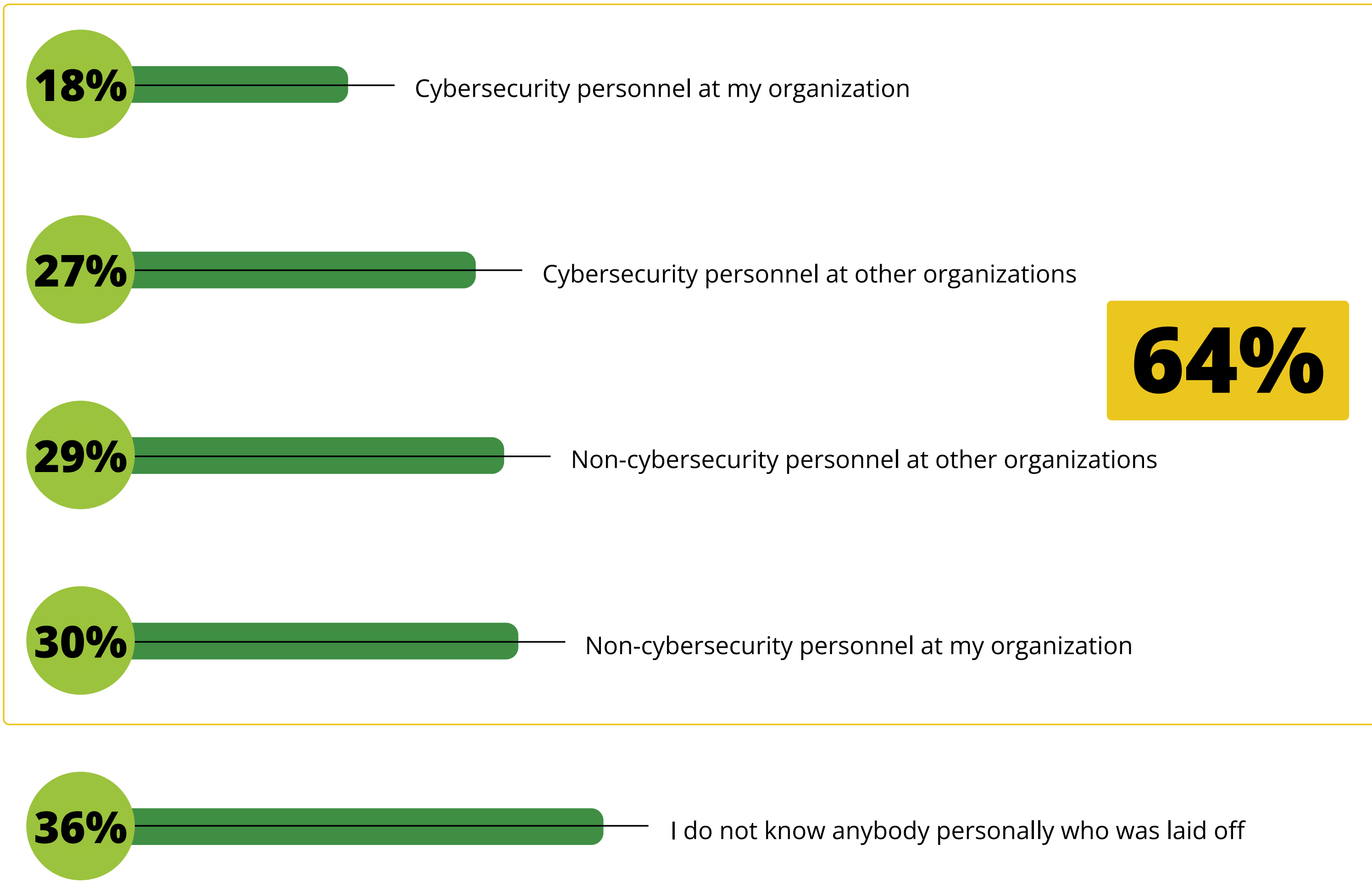
Base: 8,598-8,907 global cybersecurity professionals
Note: "Don't know/does not apply" responses were removed from the sample base.

These cutbacks are expected to continue. 31% of respondents expect there to be additional cutbacks within cybersecurity at their organization, and 70% expect those cutbacks to include layoffs. 54% expect additional cutbacks in their organizations in general, whether in cybersecurity or not.

- **Perceptions may differ from reality.** Nearly two-thirds of cybersecurity workers know someone who was laid off this year. This includes cybersecurity and non-cybersecurity workers at their own organization, along with cybersecurity and non-cybersecurity workers at other organizations (see figure 7). Seeing cybersecurity peers laid off at other organizations can significantly affect workers' perceptions of their own companies. Even if a respondent didn't know someone who was laid off from their own organization, if they knew someone who was let go from another organization this year, they were nearly three times as likely to expect to see layoffs within their own organization over the next 12 months (see figure 8).

FIGURE 7

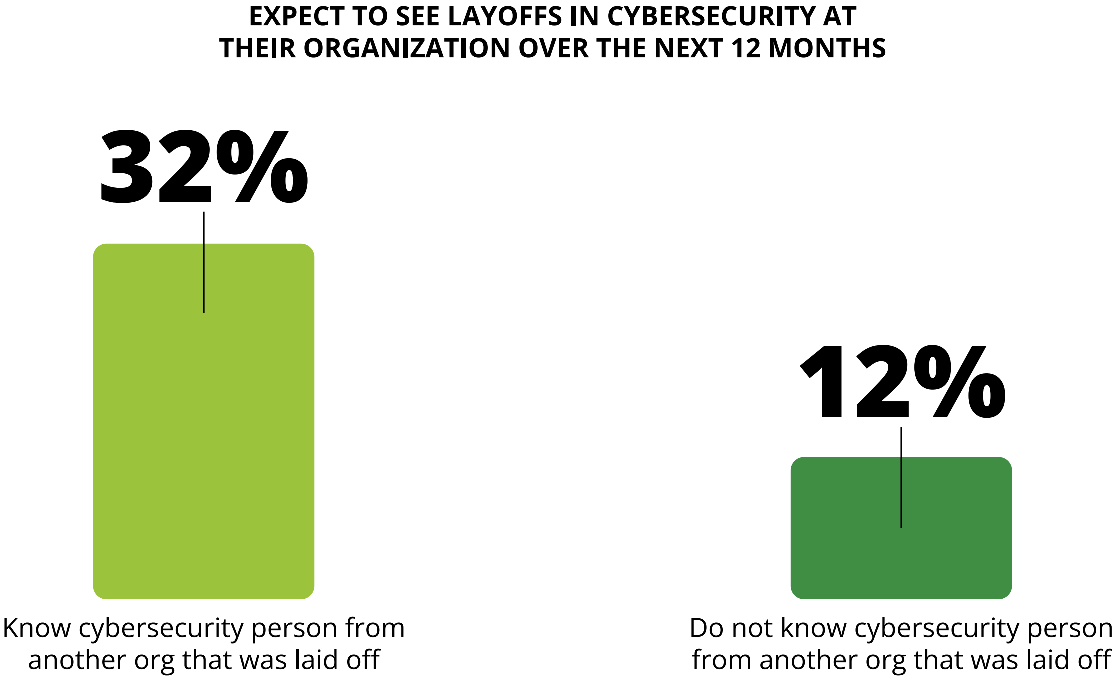
Did you know anybody personally who was laid off in the past 12 months in any of the following groups?



Base: 14,009 global cybersecurity professionals
Note: "Don't know/does not apply" responses were removed from the sample base.

FIGURE 8

Did you know anybody personally who was laid off in the past 12 months in any of the following groups?



Base: 9,676 global cybersecurity professionals who do not know a cybersecurity worker from their organization who was laid off in the last 12 months
Note: "Don't know" responses were removed from the sample base.

ORGANIZATIONS HAVE STAFFING SHORTAGES AND SKILLS GAPS BUT ARE FINDING SOLUTIONS

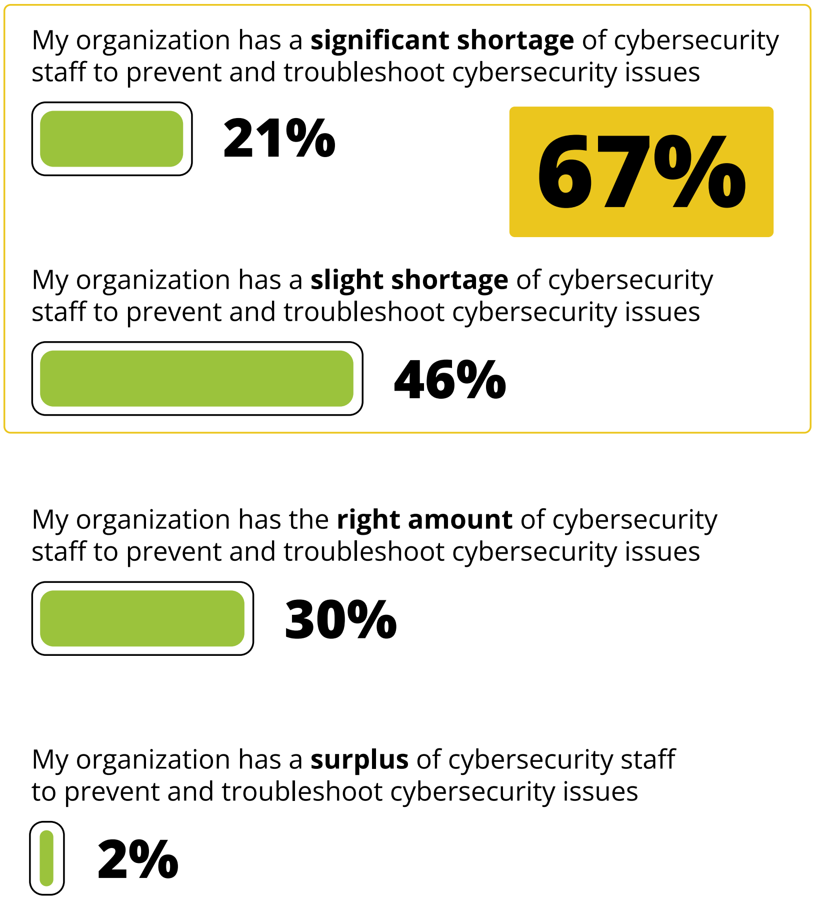
Staffing Shortages Are Expected to Get Worse but Are Also Perceived Differently Based on Seniority

Though the need for cybersecurity staff is as great as it's ever been, layoffs and cutbacks — among other factors — have caused significant staffing shortages and skills gaps within cybersecurity. We found that there's a shortage of staff to prevent and troubleshoot security issues — and a lack of budget is a common cause.

67% of respondents reported that their organizations have a shortage of the cybersecurity staff needed to prevent and troubleshoot security issues (see figure 9). Layoffs clearly play a role in this: 28% of those who have had cybersecurity layoffs report significant staffing shortages compared to 18% of those who have not had cybersecurity layoffs in the past 12 months. When asked to name the biggest cause of staffing shortages, 34% of respondents indicated a lack of budget as the leading cause, which has increased compared to 2022 (29%). Respondents were also less likely to cite problems with attrition compared to last year (27% vs. 34%) (see figure 10).

FIGURE 9

Which of the following best describes how you feel about the number of cybersecurity employees your organization currently employs to prevent and troubleshoot cybersecurity issues at your organization?



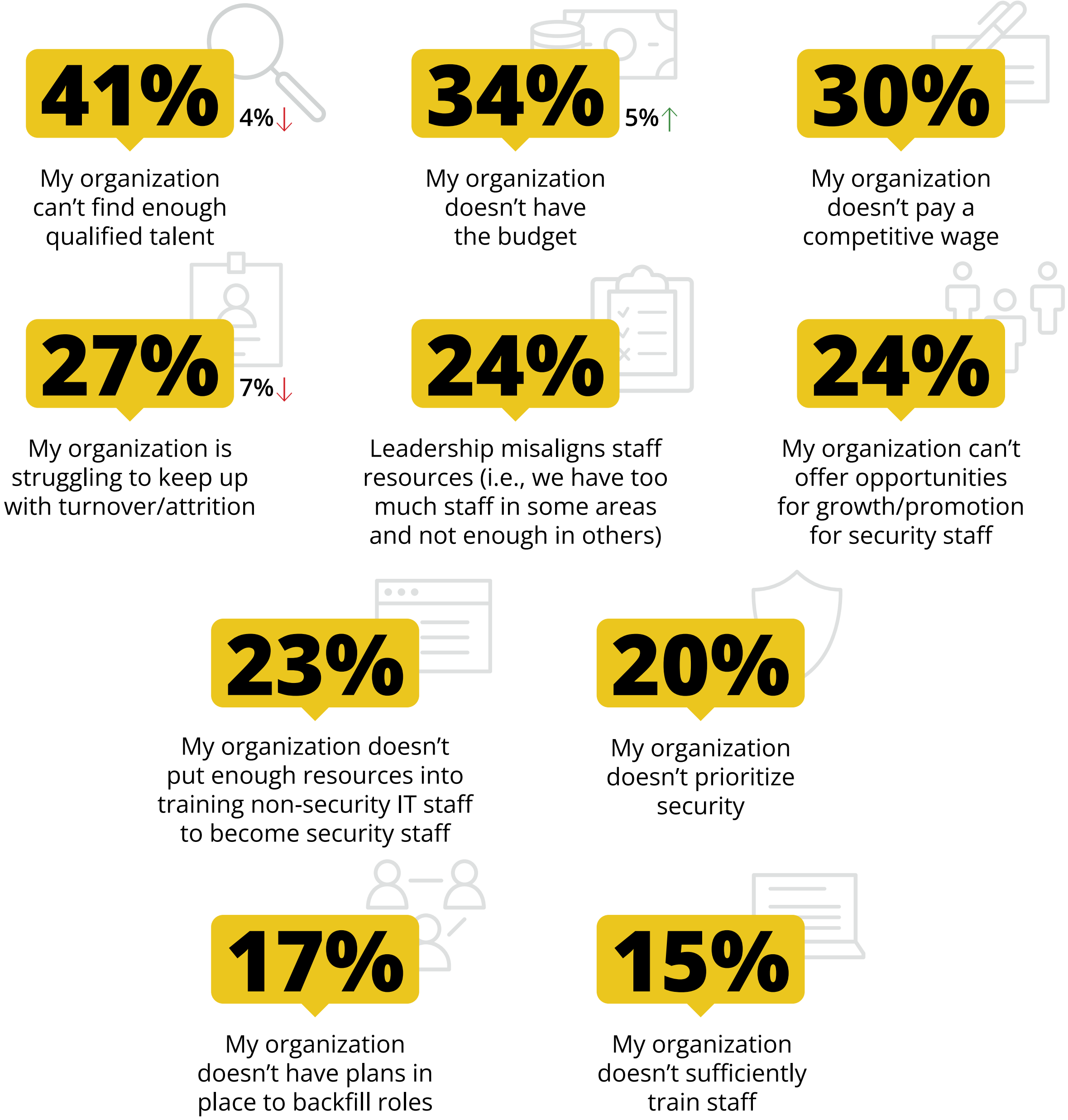
Which industries have the greatest staffing shortages?

Industry	Percentage with staffing shortages
Education	78%
Government (non-military)	78%
Non-profit	76%
Military/military contractor	76%
Aerospace	75%
Healthcare	74%
Automotive	71%
Energy/power/utilities	70%
Insurance	69%
Food/beverage/hospitality/travel	68%
Transportation	68%
Entertainment/media	67%
Manufacturing	67%
Non-security software/ hardware development	67%
Retail/wholesale	63%
Agriculture	62%
Construction	62%
Financial services	62%
Telecommunications	62%
Engineering	61%
Security software/ hardware development	60%
Hosted/cloud services	55%
Consulting	54%

Base: 8,212 global cybersecurity professionals.
Note: Percentages may not total 100 due to rounding; "Don't know/does not apply" responses were removed from the sample base.

FIGURE 10

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



Base: 5,526 global cybersecurity professionals
Note: "Don't know/does not apply" responses were removed from the sample base.

Skills Gaps Are Common but Can Be More Challenging Than Staffing Shortages

Staffing shortages (i.e., shortages in the number of total cybersecurity workers at an organization) aren't the only way that organizations can be lacking in their cybersecurity workforce. This year, we are diving into the subject of skills gaps. A skills gap is an area in which cybersecurity teams lack workers with proficiency or expertise in particular skills that are necessary to function effectively.

We have found that there is a clear and critical need to fill skills gaps in the cybersecurity profession. By identifying the areas in which these gaps exist and which skills are most desirable, we can better understand the pain points and get closer to a solution. We found that:

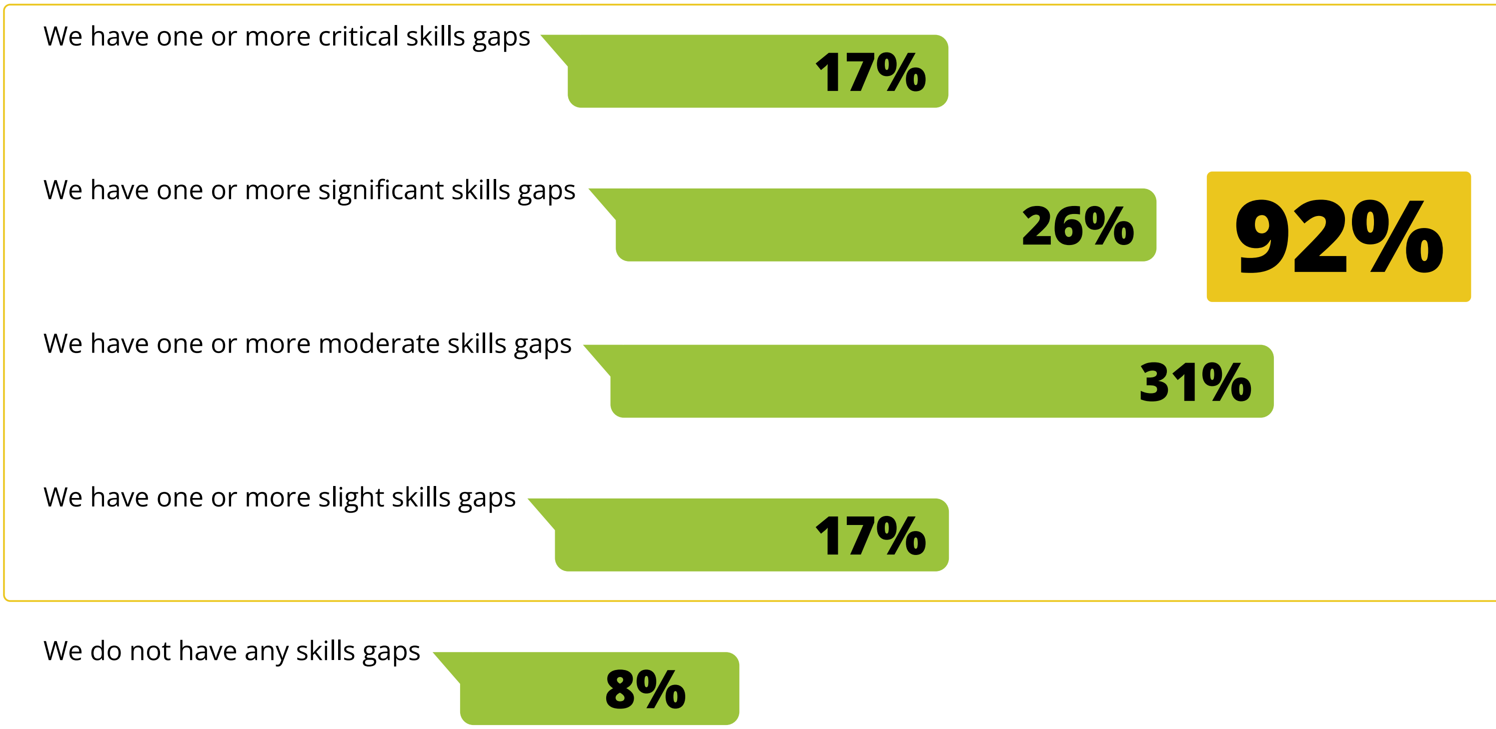
- **Nearly all organizations have cybersecurity skills gaps.** 92% of cybersecurity professionals say their organization suffers from skills gaps in one or more areas, and 43% cite one or more significant or critical skills gap at their organization (see figure 11). Skills gaps range from technical skills like penetration testing and Zero Trust implementation to non-technical skills like communication. Layoffs have an outsized effect on skills gaps. Most organizations that have had cybersecurity layoffs (51%) have been impacted by one or more significant skills gaps compared to just 39% of organizations that have not had layoffs (see figure 12). In fact, layoffs seem to have a greater effect on skills gaps than they do on total staffing shortages.

58%

believe that the negative impact of worker shortages can be mitigated by filling key skills gaps.

FIGURE 11

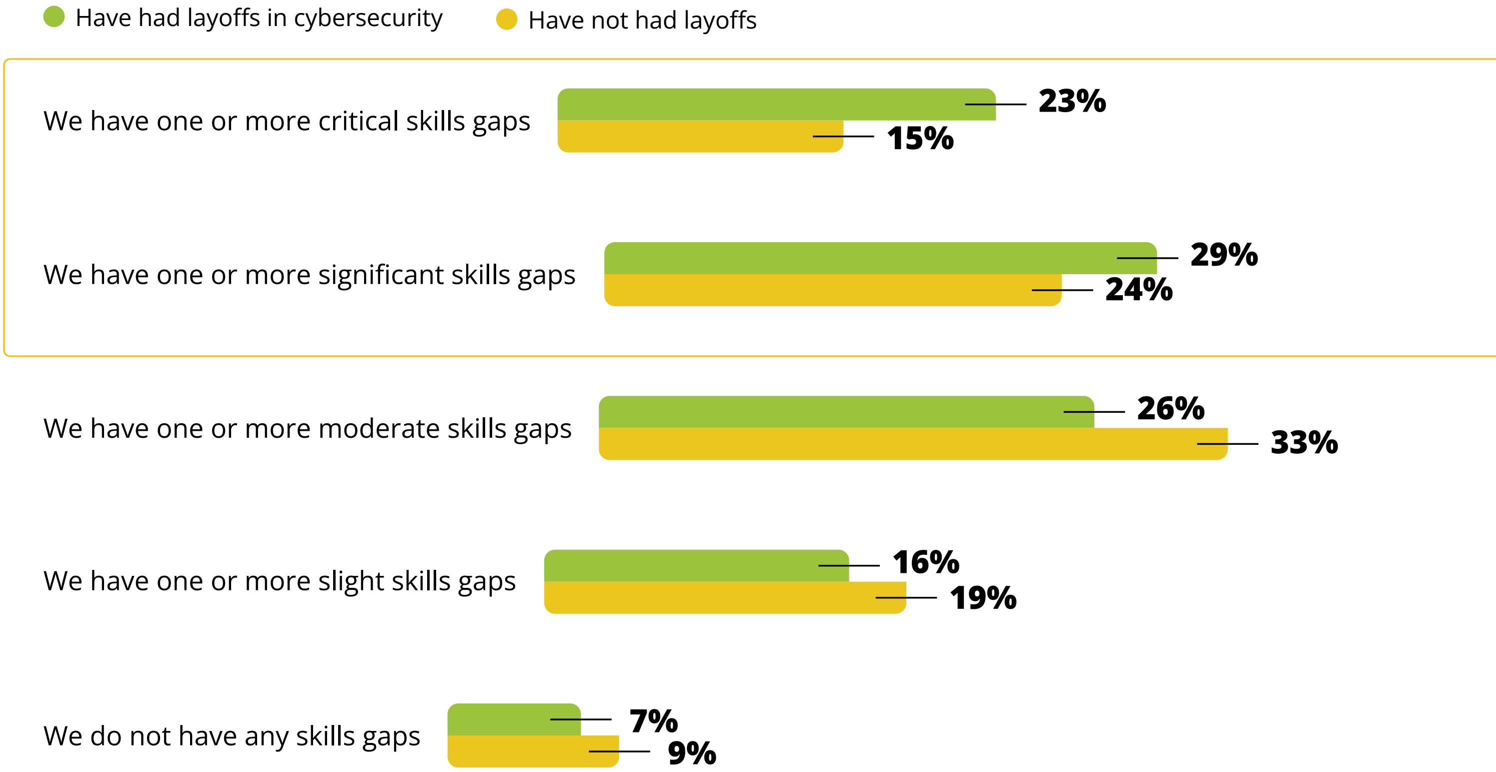
To what extent does your organization's security team have one or more skills gaps?



Base: 12,468 global cybersecurity professionals
Note: "Don't know/does not apply" responses were removed from the sample base; Total percentages may not equal separate values due to rounding.

FIGURE 12

To what extent does your organization’s security team have one or more skills gaps?

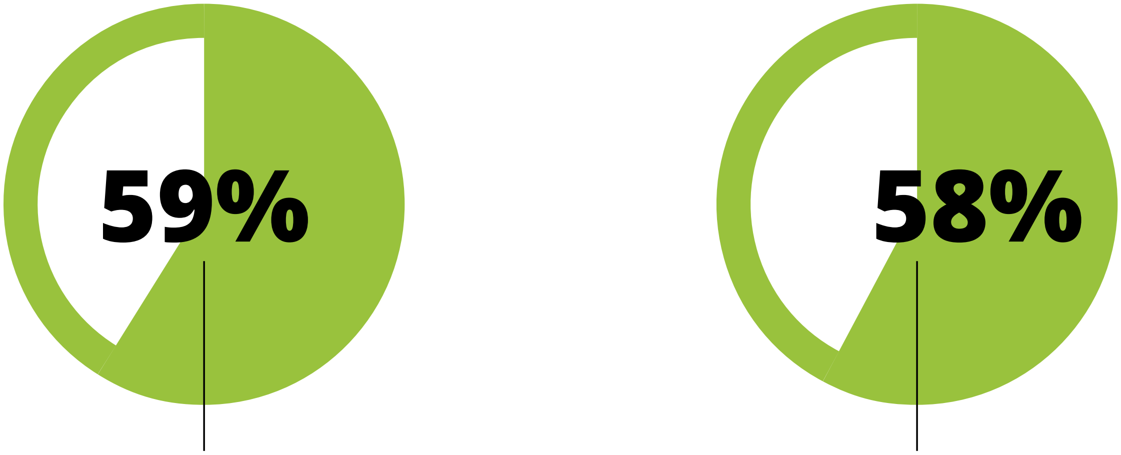


Base: 7,900 global cybersecurity professionals
Note: “Don’t know/does not apply” responses were removed from the sample base.

- **Skills gaps are often worse than shortages.** Organizations may have a number of cybersecurity workers, but if those workers all lack certain critical skills, that surplus of headcount can be completely negated. 59% of cybersecurity workers said that skills gaps can be worse than total worker shortages. This number is even higher (67%) among workers whose organization actually has *both* skills gaps and total staffing shortages (see figure 13).

FIGURE 13

To what extent do you agree or disagree with the following statements about hiring and recruiting cybersecurity roles at your organization?



59% of respondents agree/strongly agree that "**Skills gaps can be worse than total worker shortage gaps.**"

58% of respondents agree/strongly agree that "**We can help mitigate worker shortages if we have efficient distribution of skills across the team.**"

Base: 13,105-13,148 global cybersecurity professionals
Note: "Don't know/does not apply" responses were removed from the sample base.

67% of those whose organizations have both skills gaps and worker shortages agree that skills gaps can be worse than total worker shortages compared to 52% of those who have neither.

The survey also revealed opportunity here, as 58% of respondents also believe that the negative impact of worker shortages can be mitigated by filling key skills gaps. This places critical priority on identifying and taking action to educate employees in vital areas of cybersecurity knowledge or providing reimbursements to explore external professional development or third-party certifications/education.

- **Recruiting issues and lack of strategic budgeting also drive skills gaps.** The two most common reasons for skills gaps cited by respondents were the inability to find the people with the skills they need and the struggle to keep people with in-demand skills due to low wages, lack of promotion opportunities, etc. (see figure 14). Offering sufficient compensation plays a big role here: 58% of cybersecurity workers at organizations that do not offer a competitive salary say their organization has skills gaps because they struggle to keep people with in-demand skills. In comparison, only 38% of those at organizations that pay competitive wages see skills gaps. And overall, 48% of organizations that don't offer competitive salaries have significant skills gaps, compared with 31% of those organizations that do offer competitive compensation.

48%

of respondents at organizations that don't offer competitive salaries have significant skills gaps, compared with

31%

of those organizations that do offer competitive compensation.

FIGURE 14

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

(Showing top nine ranked responses)

44%
My organization can't find people to hire with the skills we need

42%
In general, we struggle to keep people with in-demand skills (e.g., due to low wages, lack of promotion opportunities, etc.)

41%
My organization doesn't have the budget to hire enough people

36%
Leadership misaligns staff resources (i.e., too much staff in some areas and not enough in others)

33%
My organization doesn't put enough resources into training non-security IT staff to become security staff

32%
People with these skills recently quit, and we haven't replaced them

31%
My organization doesn't sufficiently train staff

25%
People with these skills recently were laid off, and we haven't replaced them

Base: 12,011 global cybersecurity professionals
Note: "Don't know/does not apply" responses were removed from the sample base.

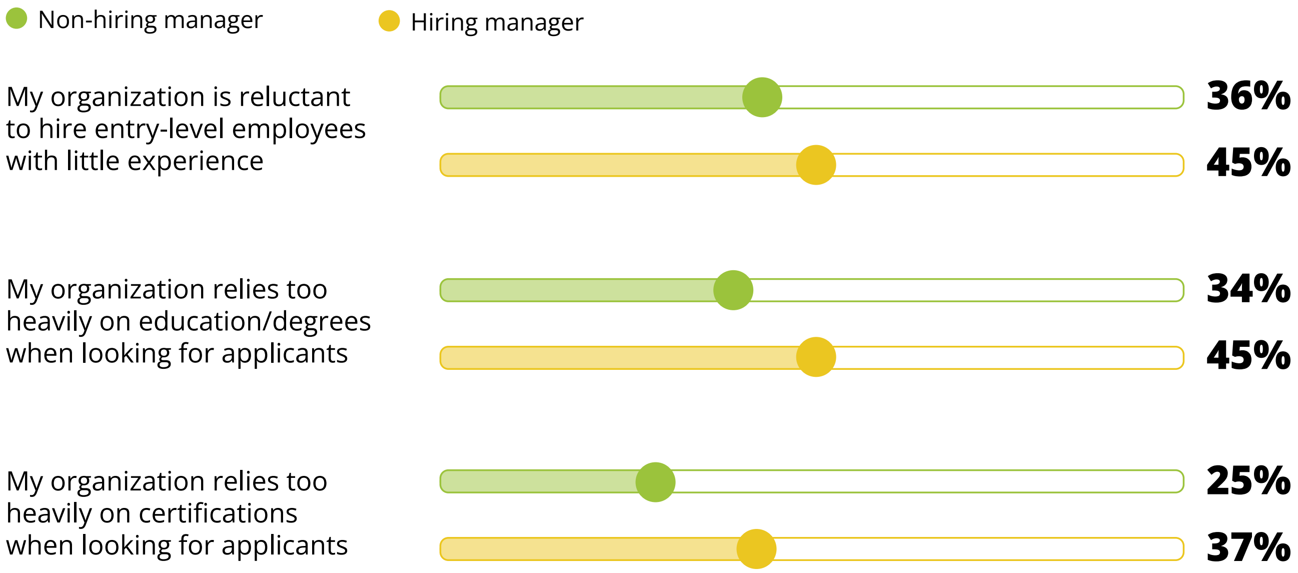
- **Cybersecurity hiring managers are held back by their organizations' policies.** Times of economic uncertainty present a critical opportunity for organizations to encourage new pathways for cybersecurity careers while filling skills gaps. Respondents cite a lack of training resources for non-security IT staff to become cybersecurity professionals (33%) as another top cause of skills gaps at their organizations. In the New Career Pathways section of this paper, we highlight how more technically experienced professionals with no prior cybersecurity experience are interested in joining the profession. These motivated professionals are applying for positions and joining cybersecurity teams, but some organizations are still too reluctant to broaden their hiring scope.

Cybersecurity hiring managers are more likely to agree than non-hiring managers that their organizations are too reluctant to hire certain types of employees. Roughly half (45%) say that they are too reluctant to hire entry-level employees or that they rely too heavily on education/degrees when looking for applicants (45%) (see figure 15).

FIGURE 15

To what extent do you agree or disagree with the following statements about hiring and recruiting cybersecurity roles at your organization?

(Showing Somewhat/Completely agree responses)



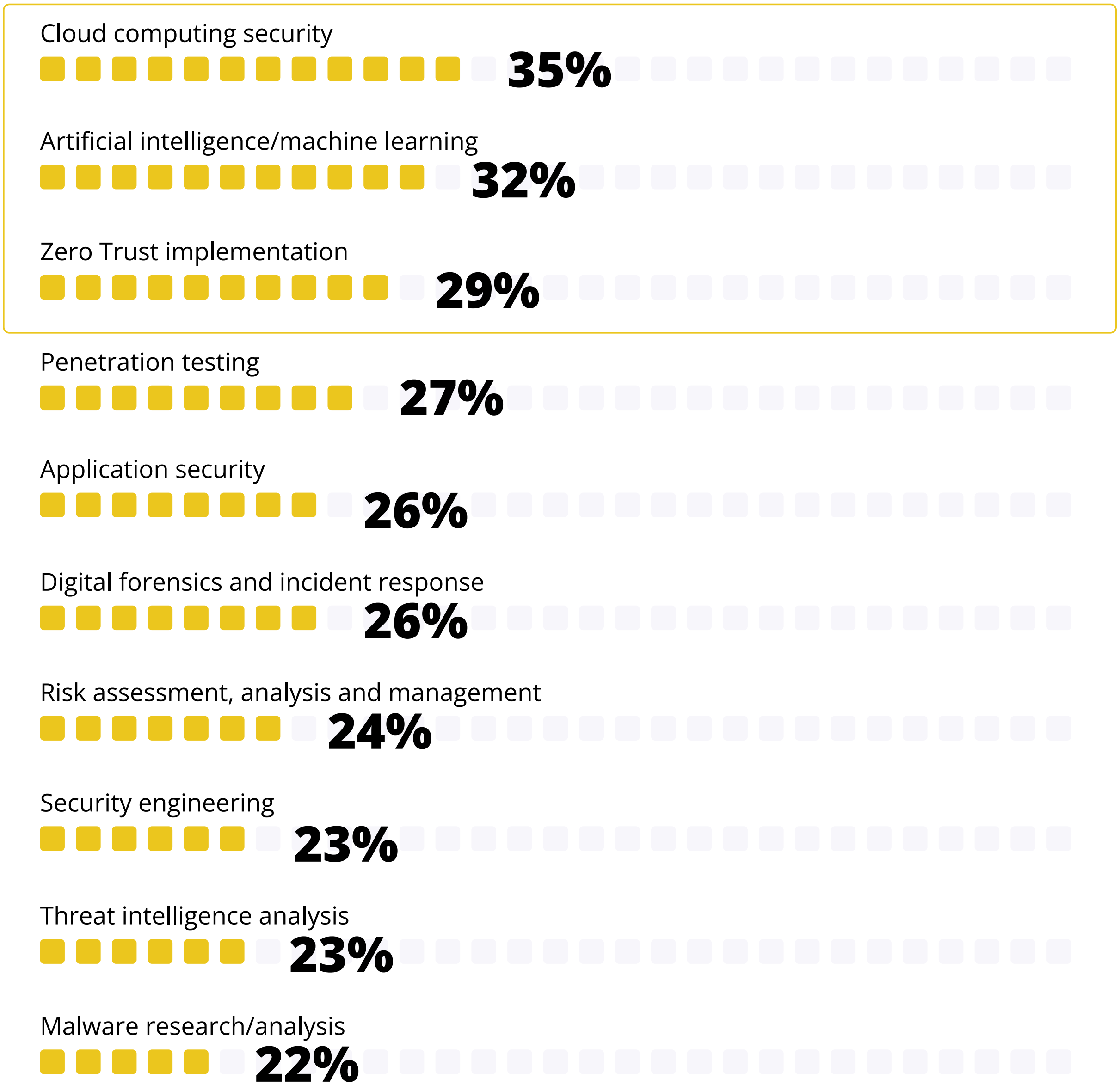
Base: 14,009 global cybersecurity professionals
Note: "Don't know/does not apply" responses were removed from the sample base.

- **Skills gaps are most common in critical areas.** We found that the most common skills gaps tend to be in areas that are gaining importance in the cybersecurity world. Cloud computing security, artificial intelligence and machine learning security and Zero Trust implementation are the current top three most common skills gaps (see figure 16).

FIGURE 16

You indicated that your organization’s security team has one or more skills gaps. Where are these gaps?

(Showing top ten responses)



Base: 11,473 global cybersecurity professionals
Note: Showing top ten responses; “Don’t know/does not apply” responses were removed from the sample base.

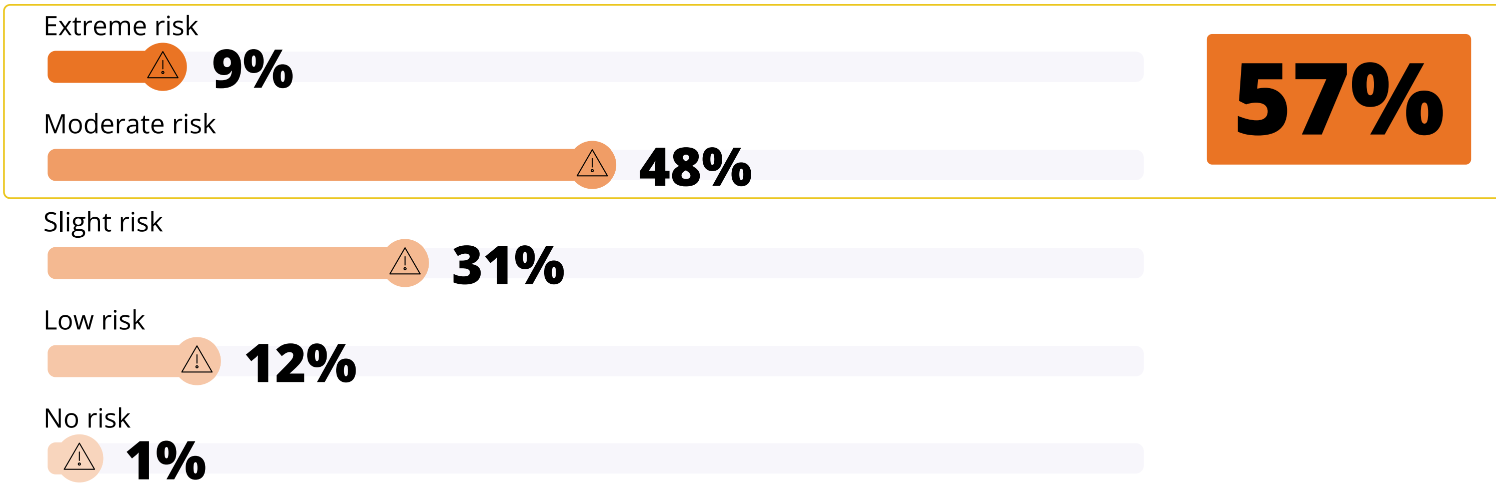
Not Surprisingly, Staffing and Skills Shortages Create Risks for Organizations

Cutbacks, staffing shortages and skills gaps have created a perfect storm, increasing risk across all industries. But what are these risks? We found that:

- **Cybersecurity staffing shortages pose a significant threat to organizations.** 57% of workers say shortages at their organization put them at a moderate or extreme risk of cybersecurity attacks (see figure 17). This is due to staffing shortages that decrease their ability to perform critical, careful risk assessment and remain agile amid a challenging threat landscape (see figure 18).

FIGURE 17

In your opinion, to what degree does this shortage of cybersecurity staff put your organization at risk of experiencing a cybersecurity attack?

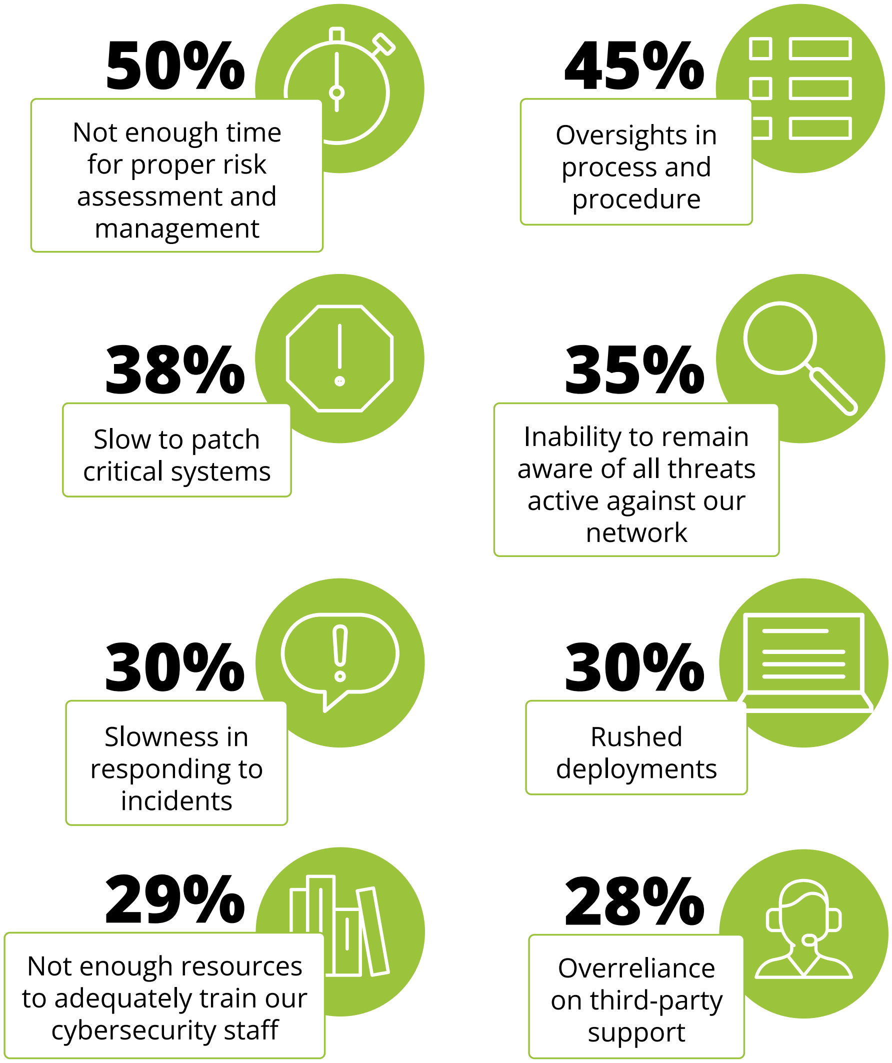


Base: 5,437 global cybersecurity professionals
Note: "Don't know/does not apply" responses were removed from the sample base; Percentages may not total 100 due to rounding.

FIGURE 18

Which of the following have you experienced that you feel would have been mitigated if you had enough cybersecurity staff?

(Showing top ten responses)



75%

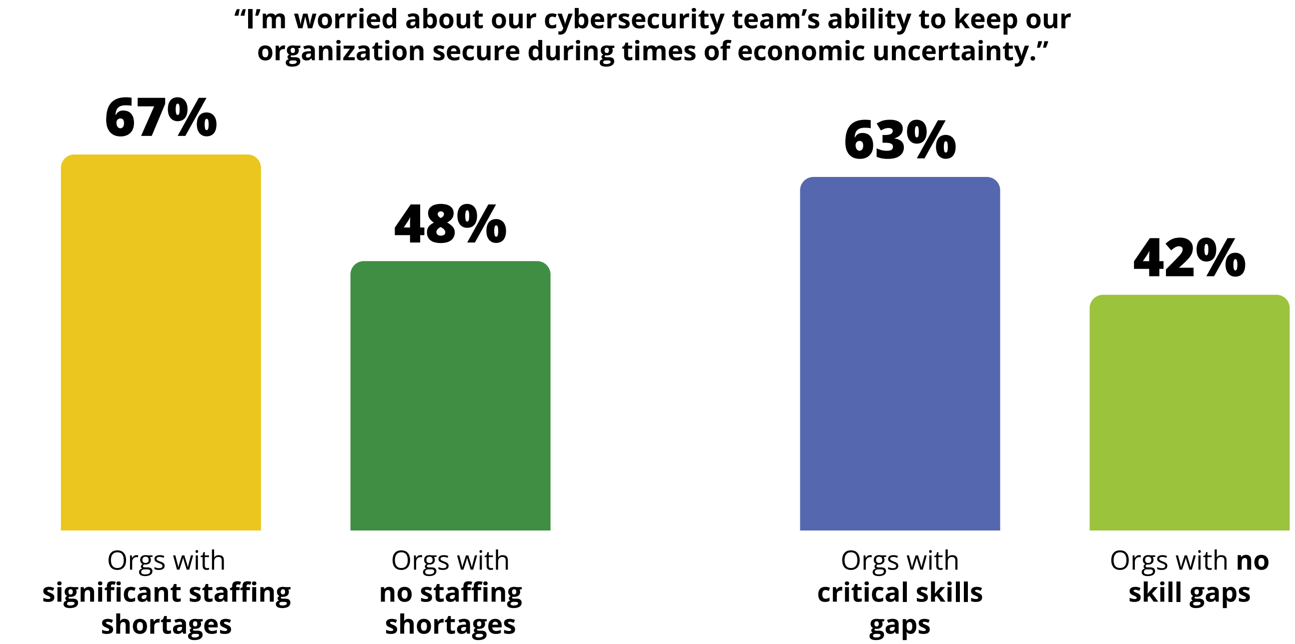
said the current threat landscape is the most challenging it has been in the past five years.

Base: 5,526 global cybersecurity professionals who reported staff shortages.
Note: "Don't know/does not apply" responses were removed from the sample base

- **Economic uncertainty reduces cybersecurity confidence.** Periods of economic uncertainty pose threats of their own: 52% of respondents are worried about their cybersecurity teams' ability to keep their organization secure — and those with staffing shortages and skills gaps are especially worried (see figure 19).

FIGURE 19

How strongly do you agree with the following statements related to the state of cybersecurity work?



Base: 2,954-7,861 global cybersecurity professionals who reported staff shortages
Note: "Don't know/does not apply" responses were removed from the sample base.

What It Means for Organizations

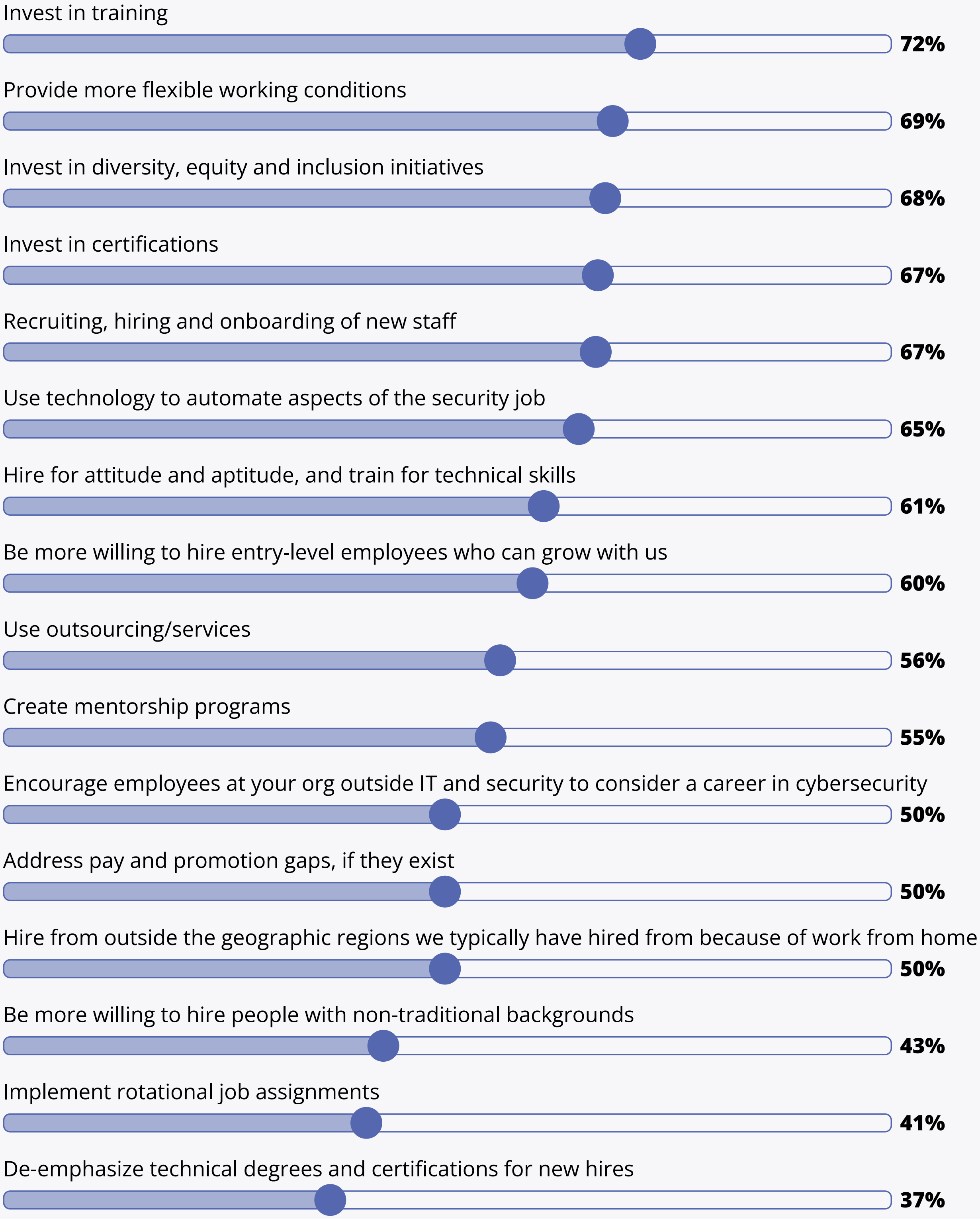
Targeted Upskilling and Working Culture Improvements Mitigate Risks Stemming from Staffing and Skills Shortages

Despite these challenges, there are ways that organizations can mitigate cyber risks stemming from staffing shortages and skills gaps. Take the following actions to overcome these obstacles:

- **Implement initiatives to prevent or mitigate staffing shortages.** Training initiatives top this list, along with creating better working conditions and creating diversity, equity and inclusion (DEI) initiatives (see figure 20). These are aimed at attracting and retaining top talent and upskilling workers in-house.
- **Upskill existing workers.** Upskilling workers is important, especially during times of economic uncertainty when many organizations face hiring freezes. Training initiatives can mitigate staff shortages by distributing skills and preventing significant skills gaps. In fact, we found that organizations investing in training today are only half as likely to have critical skills gaps as those that aren't investing and have no plans to. On the flip side, we found that outsourcing services had little to no effect on mitigating staffing shortages. It was the only initiative where those who implemented it were more likely to have staffing shortages than those who hadn't. This seems to be a trend, as last year we observed the same result.
- **Be aware of workers' worries.** We found that nearly 65% of entry- and junior-level staff expected the number of cybersecurity workers at their organization to decrease over the next 12 months. However, the higher the seniority of the respondent, the less likely they were to expect a worker reduction in the next 12 months (see figure 21). It's important for cybersecurity leaders to understand the worries of those below them in the organizational hierarchy and make sure to communicate the company's plans for staffing in the near future.

FIGURE 20

Which of the following is your organization doing or planning to do to help prevent or mitigate cybersecurity staff shortages at your organization?



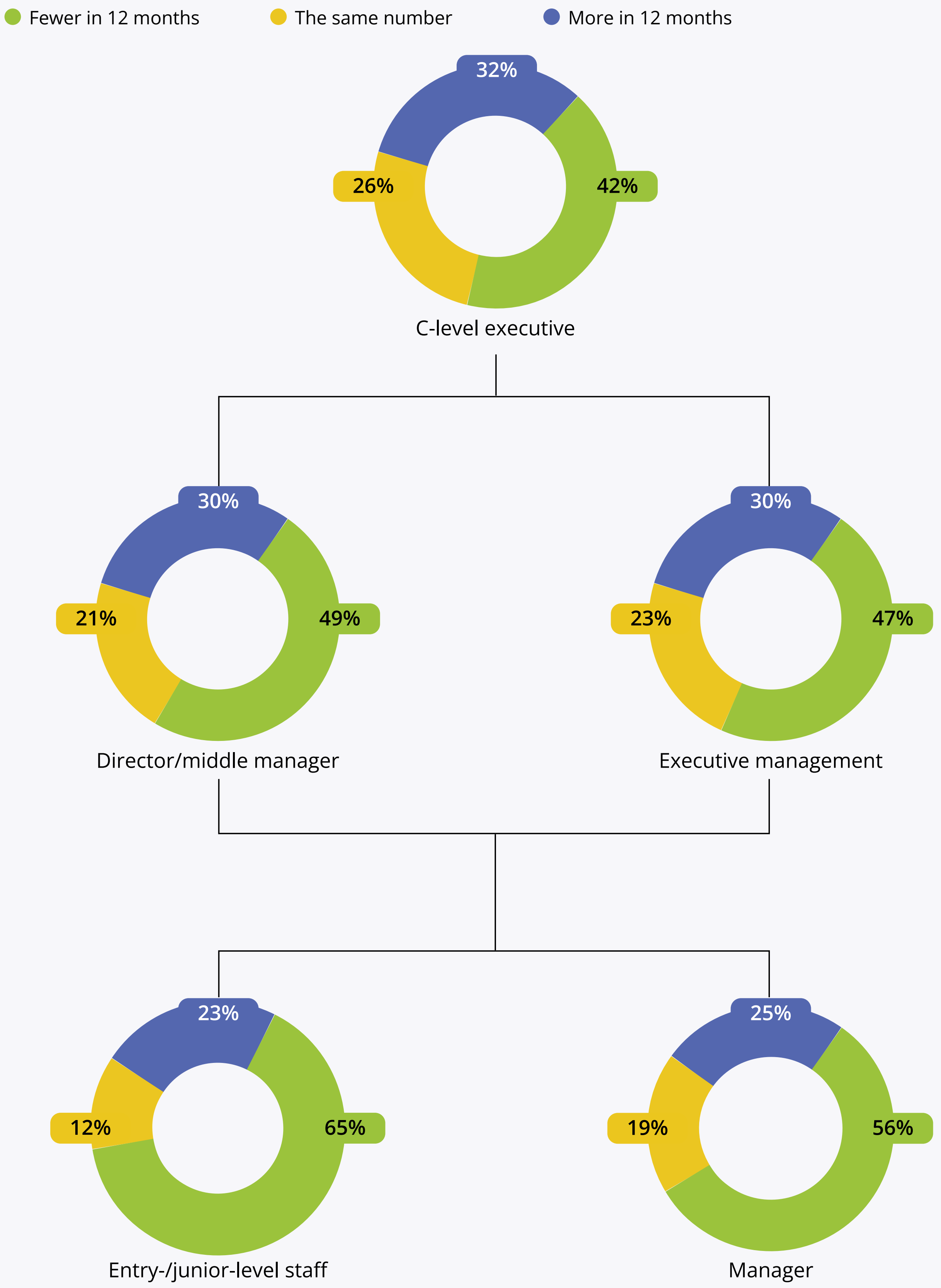
Base: 10,521-13,120 global cybersecurity professionals
Note: Showing organizations that responded with "My organization is doing this today"; "Don't know/does not apply" responses were removed from the sample base.

Organizations investing in training today are only half as likely to have critical skills gaps or significant staffing shortages as those that aren't investing and have no plans to.

FIGURE 21

Do you expect your organization to employ more, fewer or the same number of security professionals in 12 months compared to today?

(Comparing surveyed headcount to respondent's projected future headcount)



Base: 8,085 global cybersecurity professionals who reported present and expected future company size

Culture & DEI

Last year, we introduced the Employee Experience (EX) rating system to better understand what affects cybersecurity professionals' satisfaction and overall experiences. This year, we're continuing to examine culture using this system. The EX rating looks at a variety of key factors, including engagement in work, burnout rates, the sense of being fairly evaluated and more. It uses a scale from 0 (terrible) to 100 (excellent). Once evaluated, we grouped respondents into three categories based on their ratings: High EX, Medium EX and Low EX.

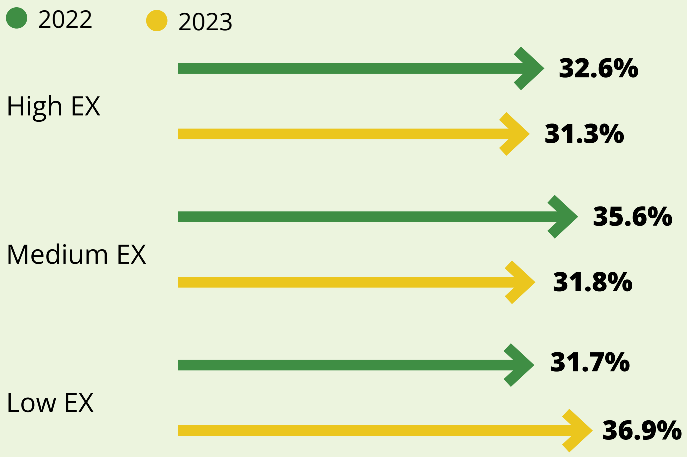
Employee Experience Rating

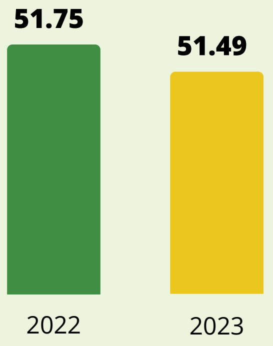
Respondents fall into three overall categories based on their employee experience levels:

		RATING	N
HIGH EX	Employees with high level of happiness at their work	62 and above	**3,822** (31.3%)
MEDIUM EX	Employees with medium level of happiness at their work	42 – 61	**4,175** (31.8%)
LOW EX	Employees with low level of happiness at their work	41 and below	**3,716** (36.9%)

- EX ratings are based on aggregated responses from a series of employee experience questions
- Ratings were indexed on a 100-point scale for ease of analysis

This year, considerably more cybersecurity professionals ended up in the Low EX bucket than last year. However, the average EX rating only dropped slightly, from 51.75 to 51.49.





Average EX rating by year

Base: 14,865 global cybersecurity professionals

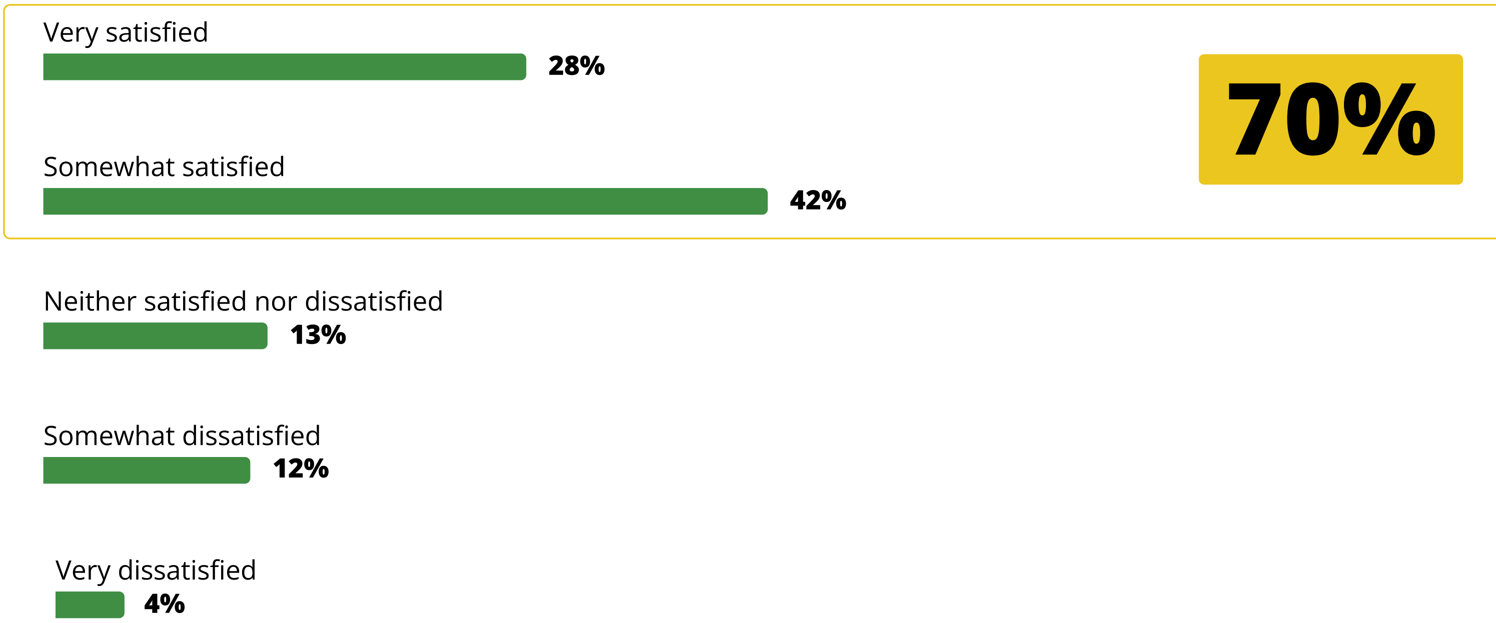
DESPITE HIGH JOB SATISFACTION, BURNOUT RISKS STEM FROM THE RIPPLE EFFECTS OF CUTBACKS, LAYOFFS AND LACK OF MANAGEMENT SUPPORT

Having a strong culture within cybersecurity is critical for organizational success. Happy workers are more motivated, more focused and are less likely to make mistakes. Building effective culture is harder than ever during times of economic uncertainty. Hiring and promotion freezes, budget cuts and layoffs loom large in workers' minds, and organizations need to scramble to keep their workers from burning out. We found that:

- **Overall job satisfaction remains high.** Despite significant turmoil, an uncertain economy and the most challenging threat landscape to date, cybersecurity workers are fairly content with their roles. 70% reported being somewhat or very satisfied in their jobs today (see figure 22). In addition, 82% say they work well with security team members, and 79% say they work well with non-cybersecurity people at their organization.

FIGURE 22

Overall, how would you rate your level of job satisfaction?



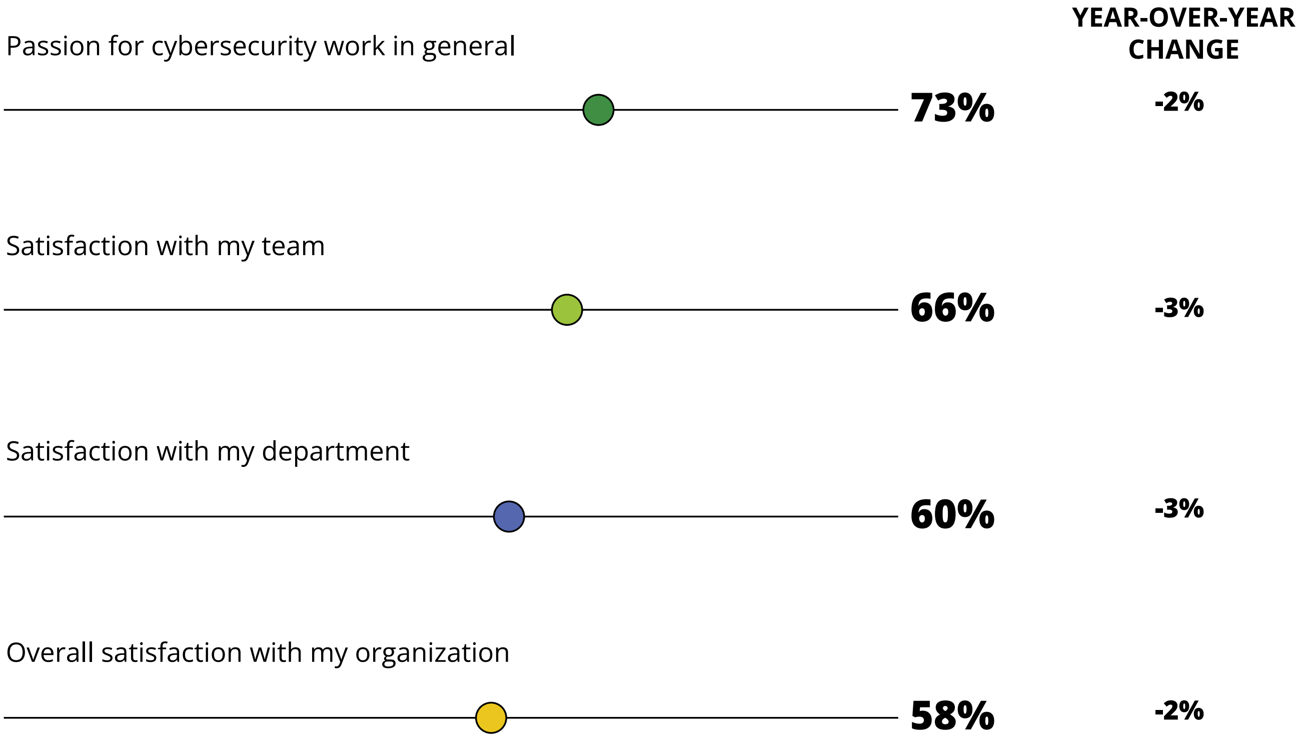
Base: 14,865 global cybersecurity professionals

- **Overall satisfaction has dipped somewhat this year.** When asking about overall job satisfaction, we saw a 4% decrease year over year — a trend that showed consistently throughout all satisfaction-related questions. Much like last year, satisfaction is higher the closer we look at the actual worker. Passion for cybersecurity work in general is highest, while satisfaction with workers' teams is slightly lower, and satisfaction with workers' departments and organizations overall are lower still (see figure 23).

FIGURE 23

Rate your feelings for each following item on a scale from very low to very high.

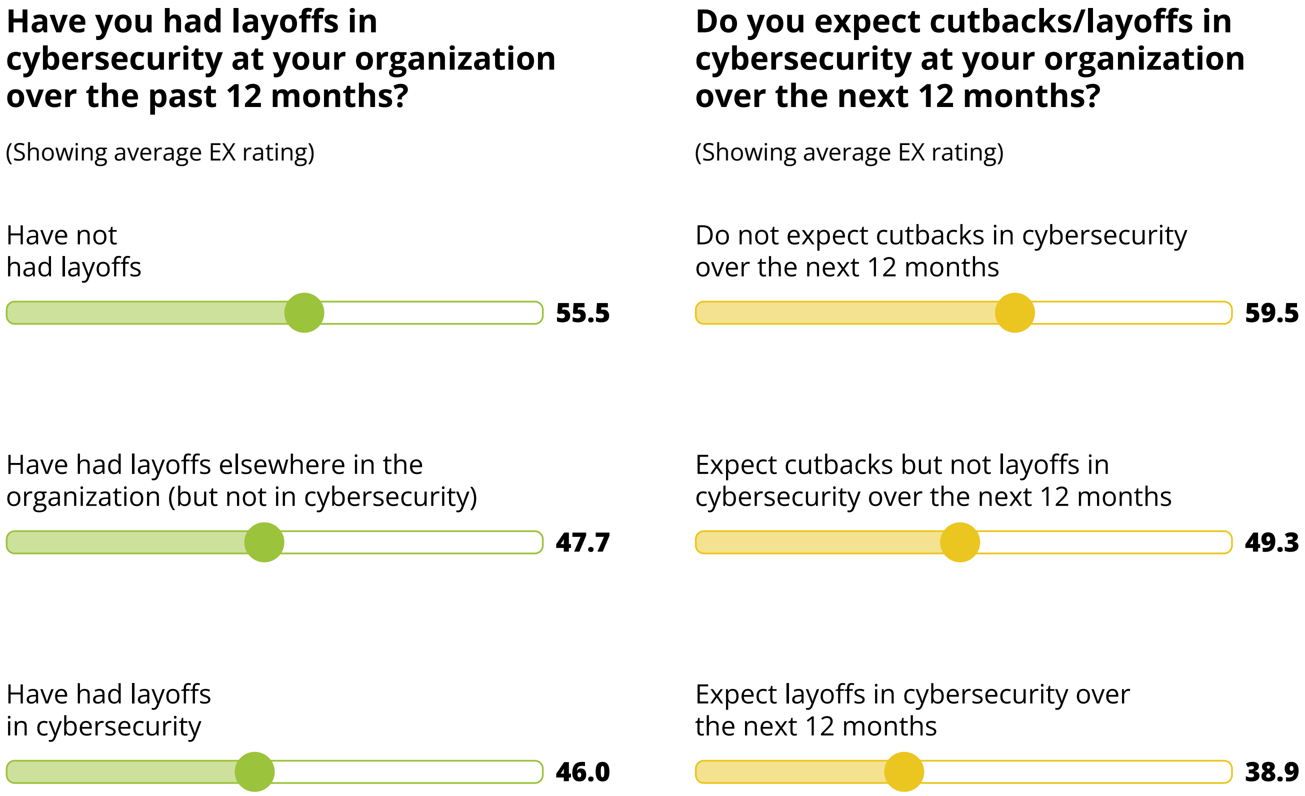
(Showing High/Very high responses)



Base: 13,815-14,574 global cybersecurity professionals
Note: "Don't know/does not apply" responses were removed from the sample base.

- **Cutbacks and layoffs have harmed morale.** As cutbacks and layoffs have increased — resulting in staffing shortages and skills gaps — satisfaction and overall worker happiness this year have dipped. Respondents whose organizations have had layoffs in cybersecurity in the past year have an average EX rating of 46.0, while those who haven't rated an average of 55.5. This is even more stark among those who expect layoffs in cybersecurity over the next 12 months. Their average EX rating is just 38.9, compared with an average of 59.5 for those who do not expect cybersecurity cutbacks at all (see figure 24). 68% of those who experienced layoffs said those layoffs significantly hurt team morale, and 62% reported that cybersecurity cutbacks have a negative effect on productivity.

FIGURE 24



Have you had layoffs in cybersecurity at your organization over the past 12 months?

(Showing average EX rating)

Do you expect cutbacks/layoffs in cybersecurity at your organization over the next 12 months?

(Showing average EX rating)

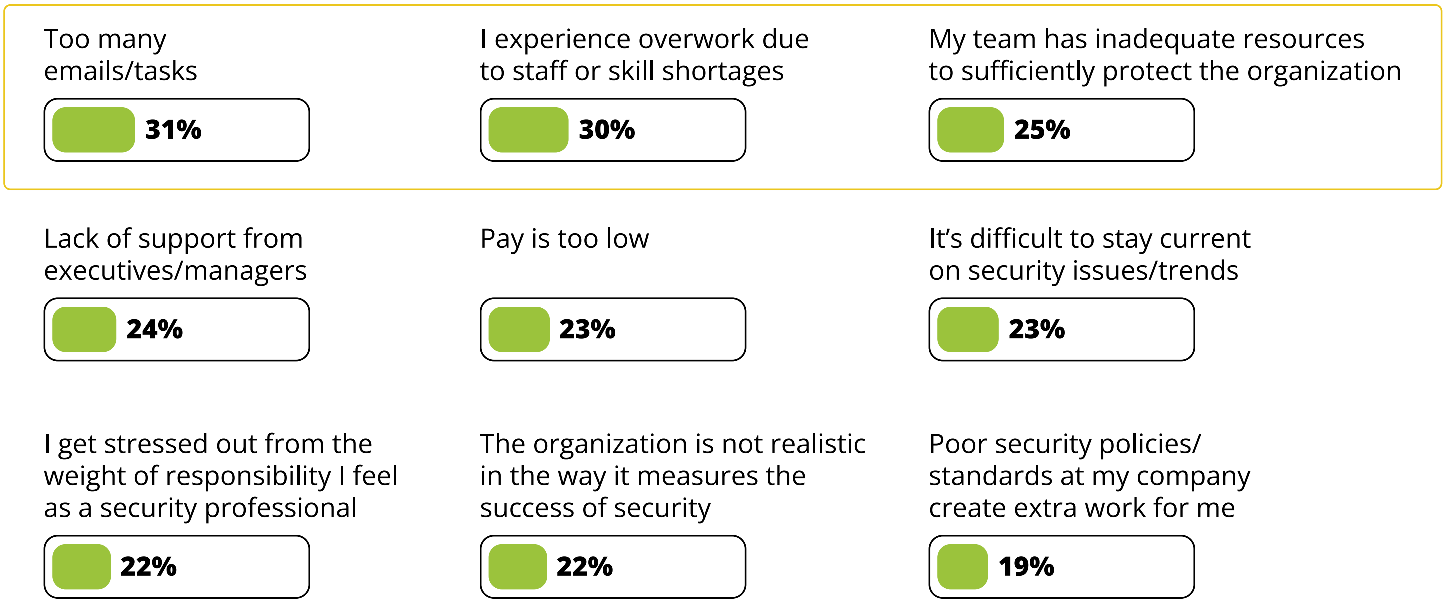
Base: 3,772-14,009 global cybersecurity professionals
Note: "Don't know/does not apply" responses were removed from the sample base

- **Layoffs and cutbacks created more work for employees.** Downsizing adds work to cybersecurity professionals' plates, hurting worker satisfaction. 71% report that cutbacks in cybersecurity resulted in an increased workload. When asked what issues negatively impact their job satisfaction, cybersecurity professionals cited an overabundance of emails and tasks, overwork due to staff or skills shortages and inadequate resources to sufficiently protect their organization — three issues related to overwork (see figure 25). These issues were significantly more common among those who have staffing shortages and skills gaps compared to those who don't (see figure 26).

FIGURE 25

Which of the following are issues in your current role that negatively impact your job satisfaction?

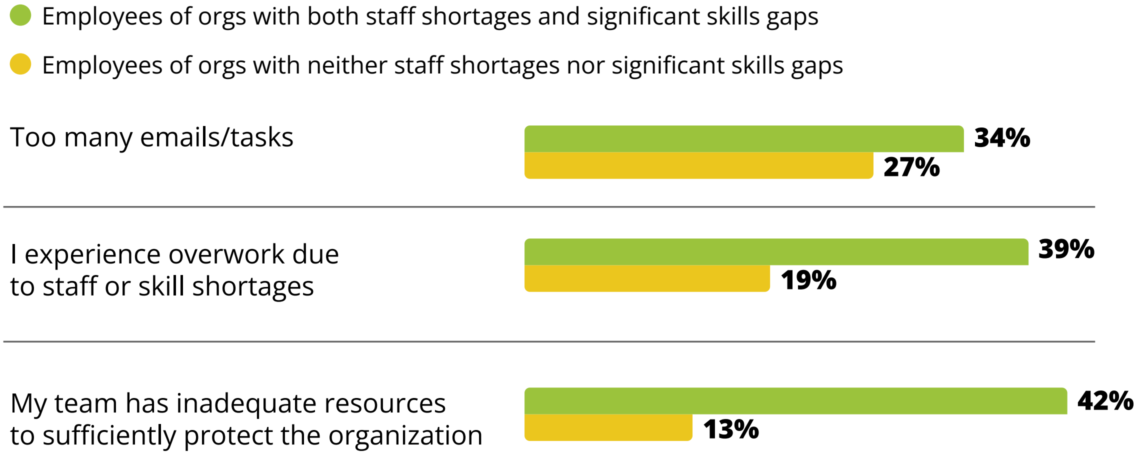
(Showing top nine responses)



Base: 14,009 global cybersecurity professionals
Note: "Don't know/does not apply" responses were removed from the sample base

FIGURE 26

Which of the following are issues in your current role that negatively impact your job satisfaction?



Base: 4,172 global cybersecurity professionals.
Note: "Don't know/does not apply" responses were removed from the sample base.

- **Organizational support impacts morale.** While issues around overwork are the most *common* problems for cybersecurity professionals, they aren't the most *impactful*. The issues that resulted in the lowest EX ratings were more likely to be related to feeling unheard, feeling unsupported by management and their expertise not being respected by their organizations (see figure 27). So while overwork has become more common, the thing that really hurts worker morale is a lack of support and respect from the organization. These were top issues last year as well, meaning it was no statistical anomaly. This is a fundamentally important issue in the cybersecurity profession.

  We found that the inverse of these issues is also true. The initiatives that create a positive work culture and result in the highest EX ratings are valuing and listening to employees' needs. Not listening to cybersecurity professionals can be a particularly harmful issue because, beyond the effect it has on employee morale, it also increases the likelihood that organizations could miss out on crucial risk-related information and put themselves at risk.

FIGURE 27

Which of the following are issues in your current role that negatively impact your job satisfaction?

LEAST NEGATIVELY IMPACTFUL ISSUES

ISSUES	AVERAGE EX RATING
It's difficult to stay current on security issues/trends	49.0
Too many emails/tasks	46.5
My team has inadequate resources to sufficiently protect the organization	44.7
Poor security policies/standards at my company create extra work for me	44.2
I experience overwork due to staff or skill shortages	43.8

MOST NEGATIVELY IMPACTFUL ISSUES

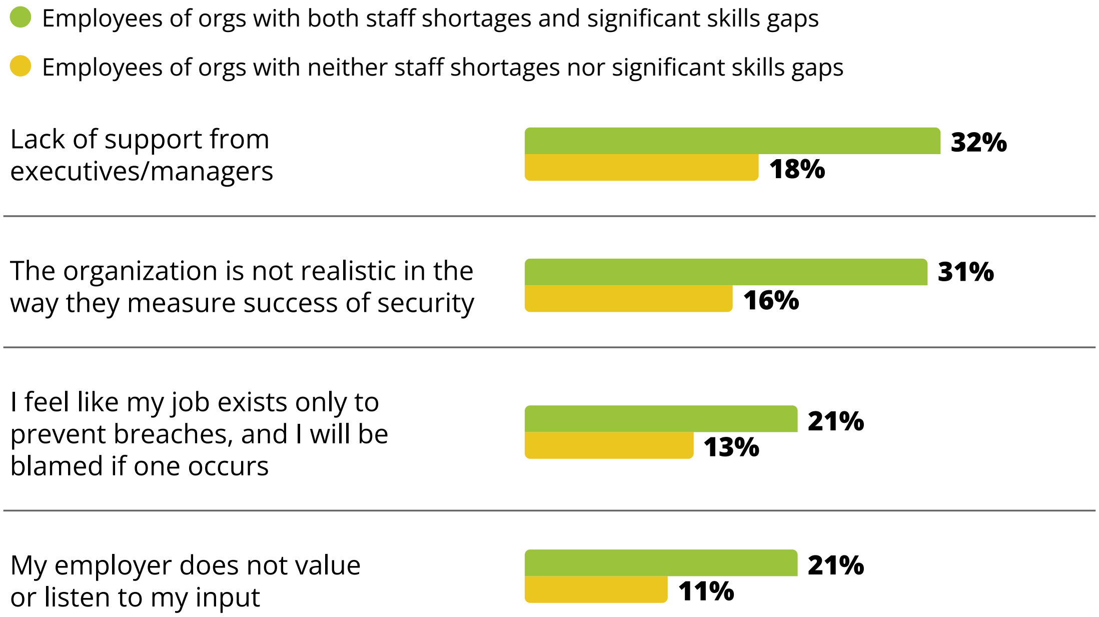
ISSUES	AVERAGE EX RATING
My employer does not value or listen to my input	36.9
Poor relationship with team members or managers	39.9
I feel like my job exists only to prevent breaches, and I will be blamed if one occurs	40.4
Lack of support from executives/managers	40.8
I am expected to work long hours	40.8

Base: 10,521-13,120 global cybersecurity professionals
Note: "Don't know/does not apply" responses were removed from the sample base

- **The wrong cybersecurity tools and resources lead to a lack of trust.** Staffing shortages and skills gaps play a surprisingly large role here as well. When cybersecurity professionals are not given the tools and resources they need to succeed, it usually leads to lost trust between management and the workforce. Those at organizations with staffing shortages and skills gaps are considerably more likely to report a lack of support from managers/executives, a feeling that their employers don't value — or even listen to — their input and more (see figure 28).

FIGURE 28

Which of the following are issues in your current role that negatively impact your job satisfaction?



Base: 4,172 global cybersecurity professionals
Note: "Don't know/does not apply" responses were removed from the sample base

AN INCREASINGLY DIVERSE WORKFORCE IS A BRIGHT SPOT, WITH ROOM TO IMPROVE DEI INITIATIVES

Last year we began to explore trends around a rapidly diversifying cybersecurity workforce, and these trends continue this year. We found that:

- **Cybersecurity is diversifying more quickly across race/ethnicity than gender.** Our data shows that the makeup of the cybersecurity workforce is changing both in gender and race and ethnicity. The biggest increase we saw by age is in non-white men. Within the US, Canada, Ireland and the UK, 70% of cybersecurity professionals 60 or older are white men. In those same countries, just 37% of those under 30 are white men. We saw this trend emerge last year, and it seems to be accelerating. 66% of security workers who entered the profession in these countries in the past 12 months are non-white (see figure 29).

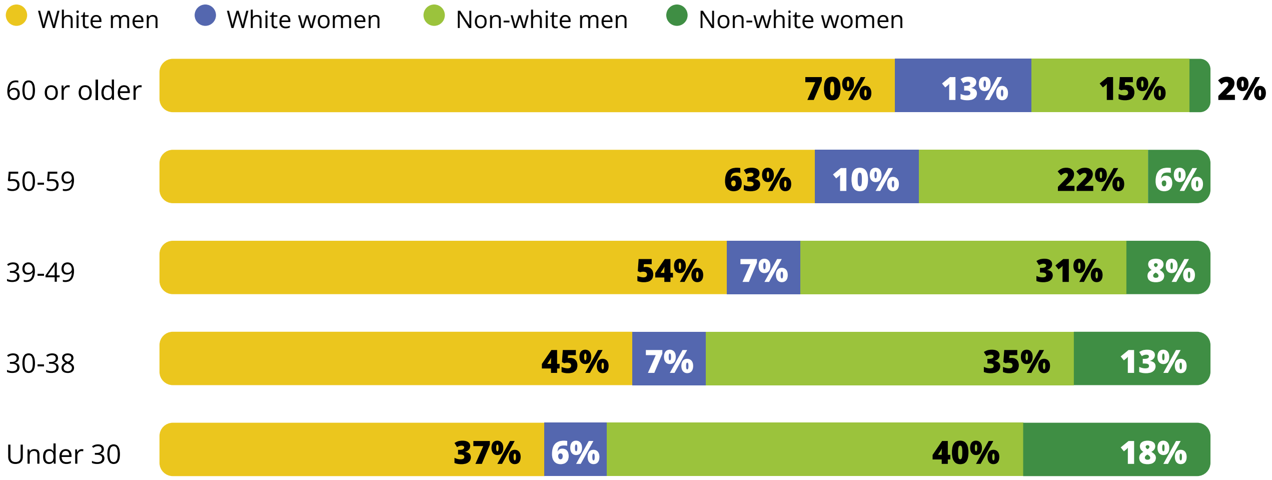
However, the change in race and ethnicity is much more significant than the change in gender. Even in the under-30 group, women represent only 26% of the cybersecurity workforce. And while this is twice as many as the 60-or-older group, it still makes up a significant minority. The pathways into cybersecurity differ by gender and race. Both women and non-white cybersecurity professionals are more likely to take an education pathway into the field and less likely to come from an IT background.

66%

of cybersecurity workers who entered the profession in the past 12 months in these countries are non-white.

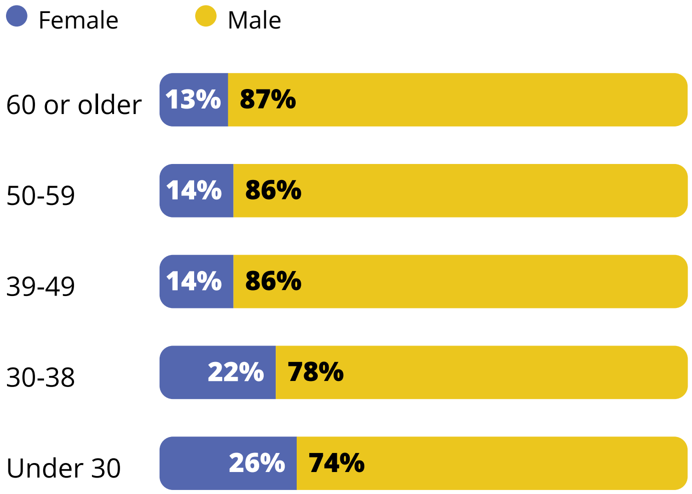
FIGURE 29

Age group by race and gender



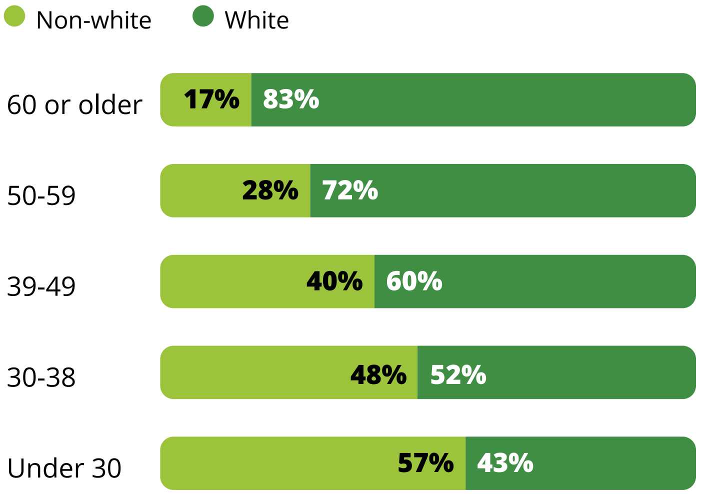
Base: 5,768 cybersecurity professionals in the United States, Canada, United Kingdom and Ireland
Note: Total percentages may not equal separate values due to rounding.

Which of the following most accurately describes you?



Base: 13,682 global cybersecurity professionals

With which of the following ethnic or cultural groups do you primarily identify?



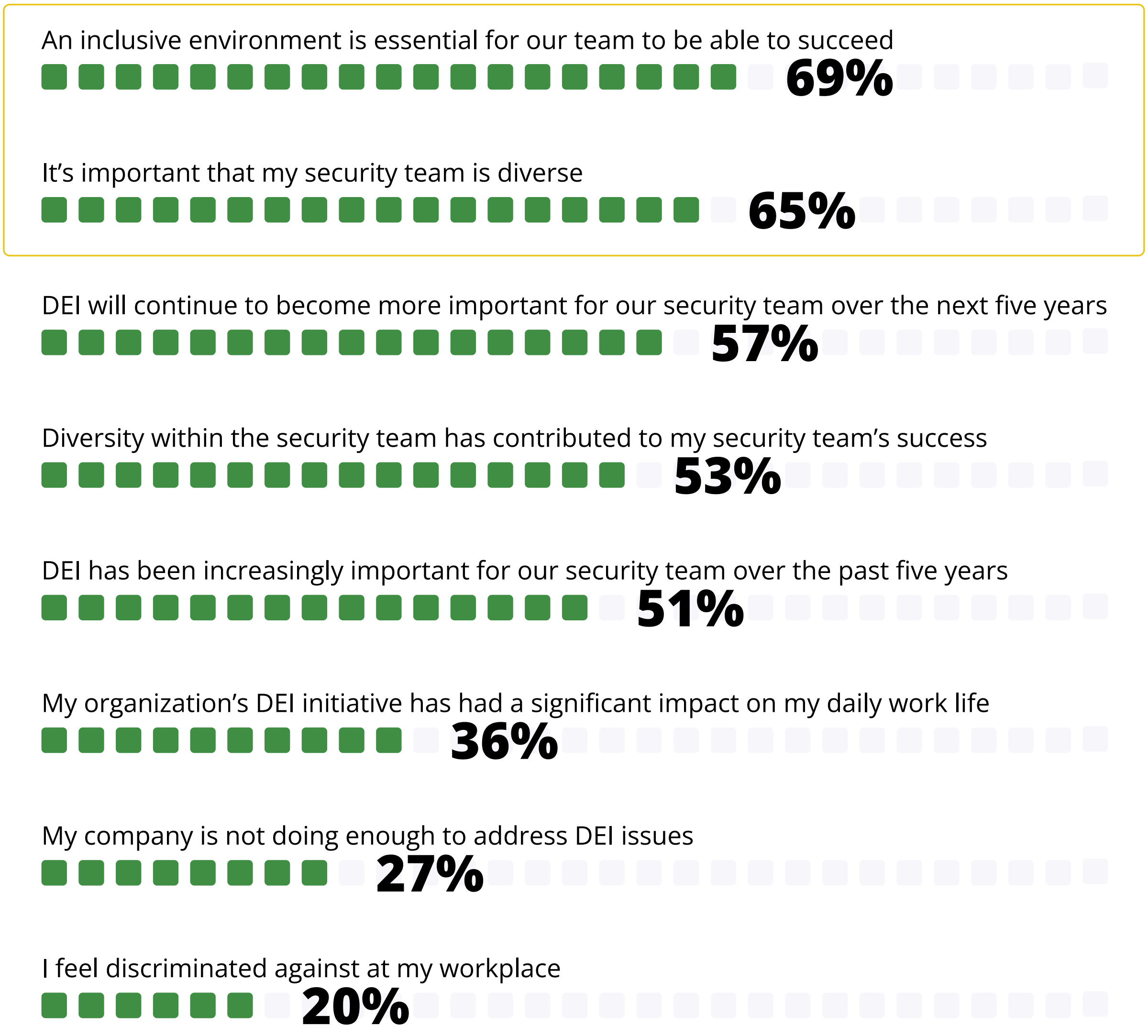
Base: 5,874 cybersecurity professionals in the United States, Canada, United Kingdom and Ireland

- **There's value in a diverse cybersecurity workforce.** Cybersecurity professionals value a diverse workforce. 69% said that an inclusive environment is essential for their team to succeed, and 65% feel that it's important that their security team is diverse. 57% say that DEI will continue to become more important for their cybersecurity team over the next five years (see figure 30). This is slightly lower than last year (62%) but still indicates a continuation of this trend.

FIGURE 30

How much do you agree or disagree with the following statements about diversity and inclusion within your organization/team?

(Showing Somewhat Agree/Completely Agree responses)

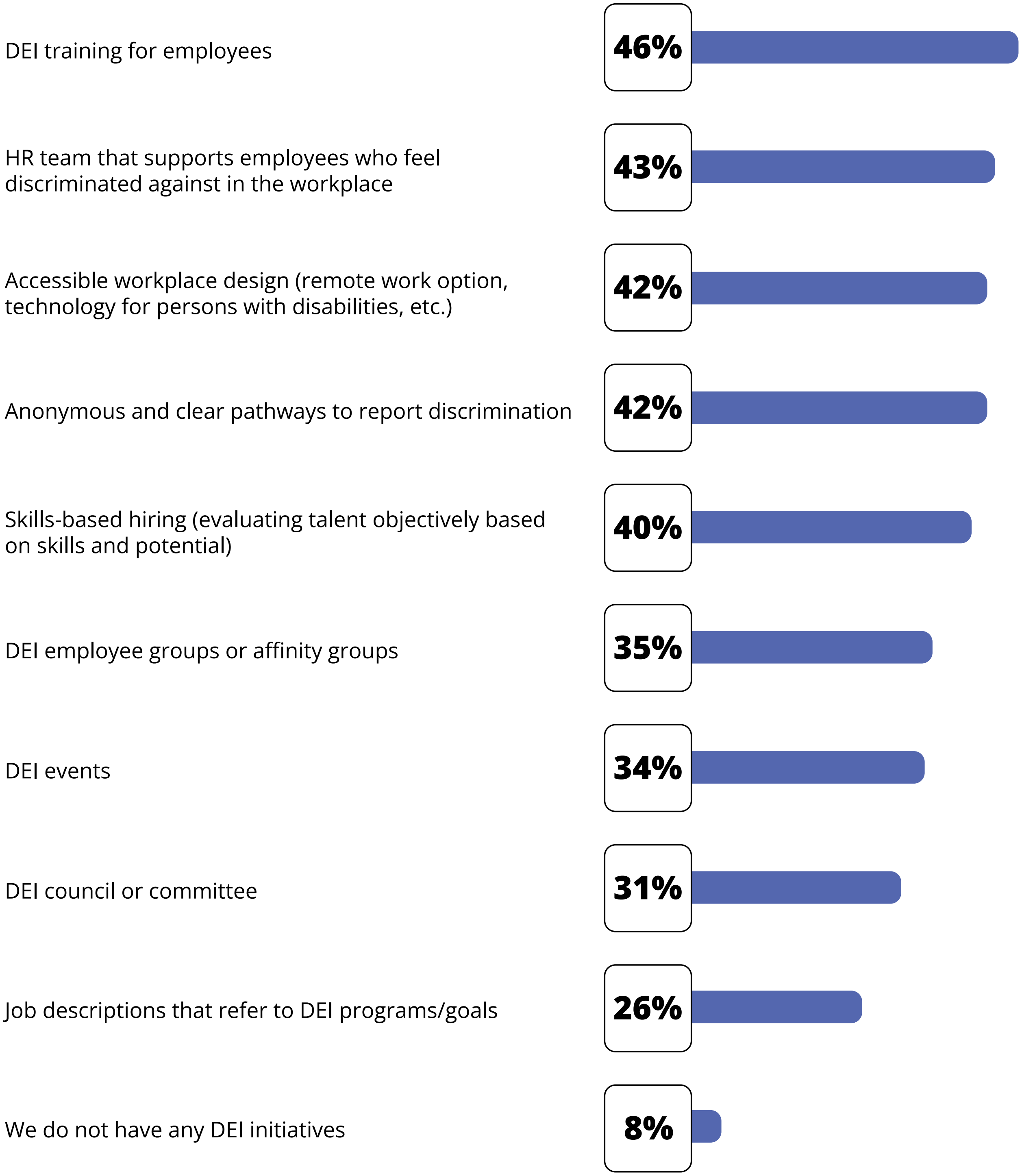


Base: 11,373-13,041 global cybersecurity professionals
Note: "Don't know/does not apply" responses were removed from the sample base

- **DEI initiatives are lacking.** However, despite cybersecurity professionals recognizing the importance of diversity, the adoption of DEI initiatives remains fairly low overall. Less than half of respondents (46%) reported that their organization currently has DEI training for employees, and 8% said that their organization does not have any DEI initiatives at all (see figure 31).

FIGURE 31

What types of programs/initiatives/tools does your company use to promote DEI and accessibility?

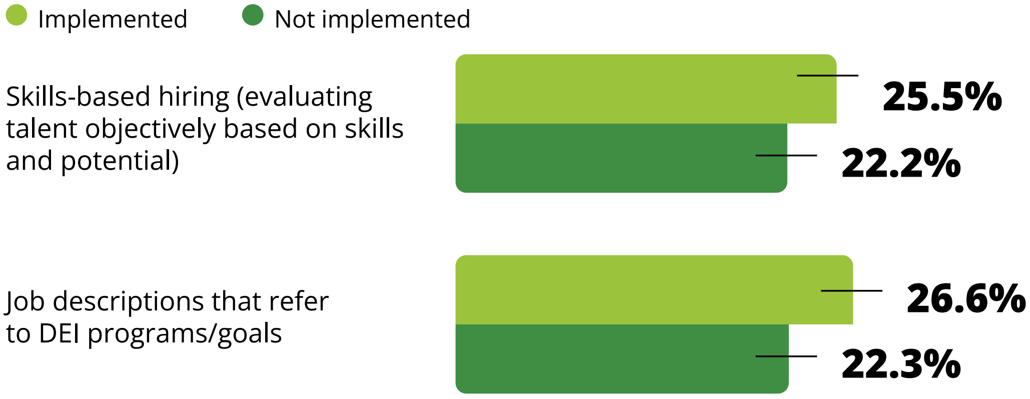


Base: 14,009 global cybersecurity professionals
Note: "Don't know/does not apply" responses were removed from the sample base

- **DEI initiatives make a significant impact, though adoption is low.** Organizations that are adopting initiatives related to hiring, such as skills-based hiring and using job descriptions that refer to DEI programs/goals, can create a more diverse workforce. Those with skills-based hiring have an average of 25.5% women in their workforces compared with 22.2% of those who have not adopted this initiative. This is also true for adding job descriptions that refer to DEI programs/goals (26.6% vs. 22.3%) (see figure 32).

FIGURE 32

Percentage of women in cybersecurity

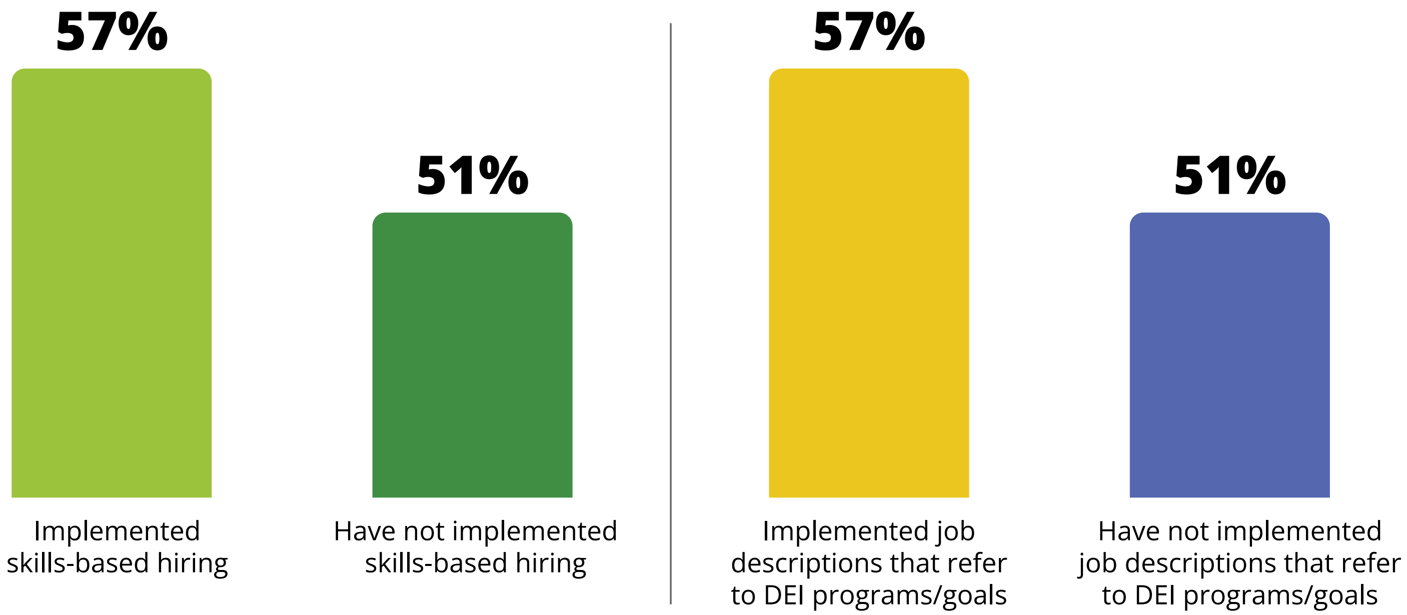


Base: 10,703 global cybersecurity professionals

DEI initiatives don't just make a difference in creating a more diverse workforce — they produce a more effective workforce as well. Cybersecurity professionals at organizations that have adopted these two DEI hiring practices were considerably more likely to feel like their organization had the tools and people they needed to ensure they are prepared to respond to cyberthreats over the next two to three years (see figure 33).

FIGURE 33

"My organization has the tools and people they need to ensure the organization is prepared to respond to cyber incidents over the next two to three years"



Base: 13,028-13,116 global cybersecurity professionals
Note: "Don't know/does not apply" responses were removed from the sample base.

What It Means for Organizations

- **Seek input and listen to feedback from employees.** We have seen consistently over the past two years that cybersecurity professionals who feel their organizations truly listen and consider their depth of expertise and knowledge as well as their preferences on working environment are far happier than those who feel unheard. Listen to your staff — don't work against them.
- **Use DEI initiatives to help navigate times of economic uncertainty.** Preventing your organization from unintentionally excluding large swaths of the available talent pool (by hiring with significant bias or creating an uninclusive environment) will be critical in ensuring that you have the right balance of skills needed to operate effectively during difficult times. In addition, the long-term effects are exceedingly valuable. A workplace where all cybersecurity professionals feel comfortable keeps workers happy, productivity high and attrition low.

New Career Pathways

80% of cybersecurity professionals agree that there are more pathways into cybersecurity today than there were in the past, and 82% agree that the increase in alternative pathways is positive for the industry. These new pathways are a product of an agile profession and the willingness of the people in it to adapt to the ever-changing and often unpredictable environment around them.

More professionals with no prior cybersecurity experience but with a more diverse technical background are applying to cybersecurity jobs. This contributes to a growing trend of experienced professionals from outside the field joining the cybersecurity industry midway through their careers, compared with a traditional wave of college graduates who have more education than on-the-job experience. This new trend helps normalize cybersecurity as a viable option for capable, experienced professionals from outside the industry looking to make a midcareer change.

This year, we offer the most detailed look ever at the career choices made by cybersecurity professionals and how they could impact the industry for generations to come. After surveying respondents of all ages and backgrounds who are charting new pathways into and throughout the profession, we found that:

- **Cybersecurity is increasingly attractive to professionals with technical, non-cyber experience.** More than half of hiring managers (59%) agree that they see an increase in job applications from technically experienced people with no prior cybersecurity experience, and organizations are embracing this. 51% say their organization is changing their hiring requirements to recruit more people from non-cybersecurity backgrounds. What's more, 56% agree that they are actively trying to recruit more of these technical professionals internally, which is also most prominent within the security software/hardware development industry (62%).

  Layoffs are an unfortunate side effect of a volatile economic environment, but with change comes opportunity. Most hiring managers (52%) agree that widespread tech layoffs give them an opportunity to get more people involved in cybersecurity (see figure 34). Layoffs can mean an abundance of skilled IT professionals hitting the job market, which creates an opportunity for cybersecurity teams who need support to hire and train them.

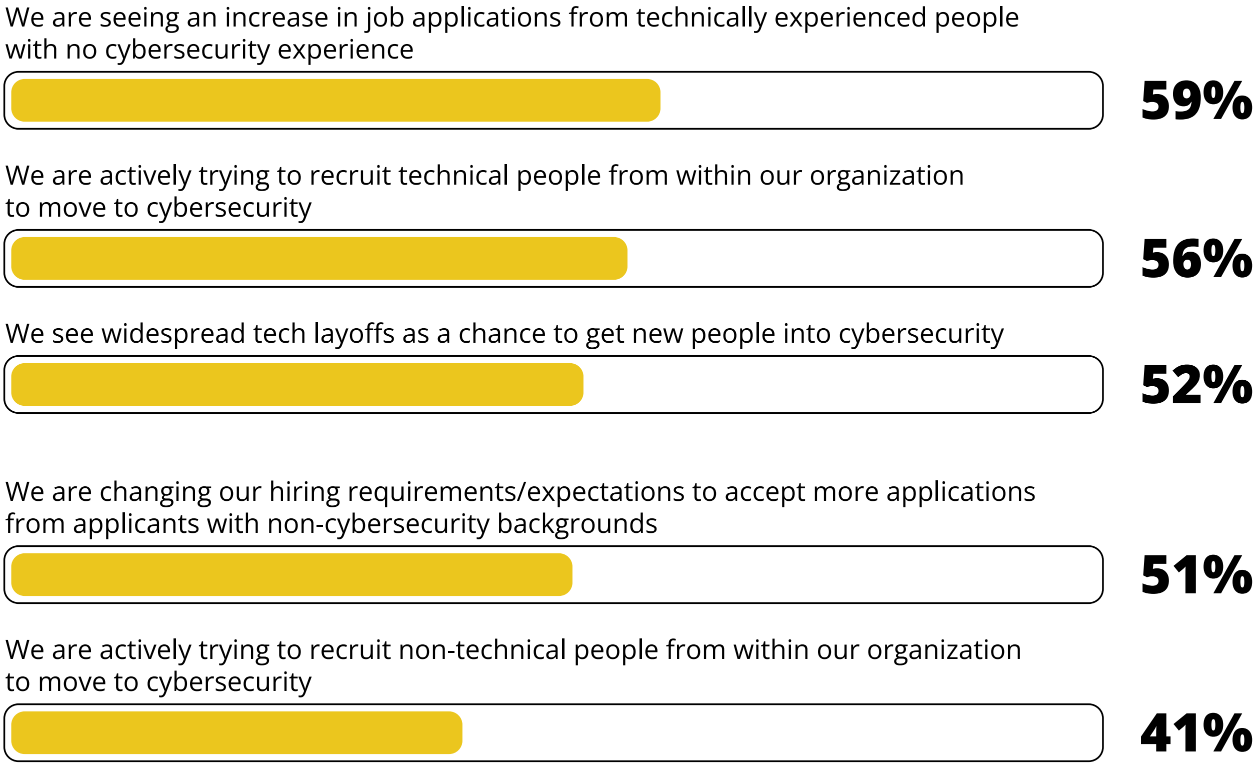
  In addition, layoffs within cybersecurity offer a chance for the industry to capitalize on the wealth of strong cybersecurity talent hitting the job market. The organizations that can pounce on hiring these people will set themselves up for success in the future.

Most hiring managers (52%) agree that widespread tech layoffs give them an opportunity to get more people involved in cybersecurity.

FIGURE 34

How strongly do you agree with the following statements related to the state of cybersecurity work?

(Showing Agree/Strongly Agree responses)



Base: 6,381-6,484 global cybersecurity professionals
Note: "Don't know/does not apply" responses were removed from the sample base.

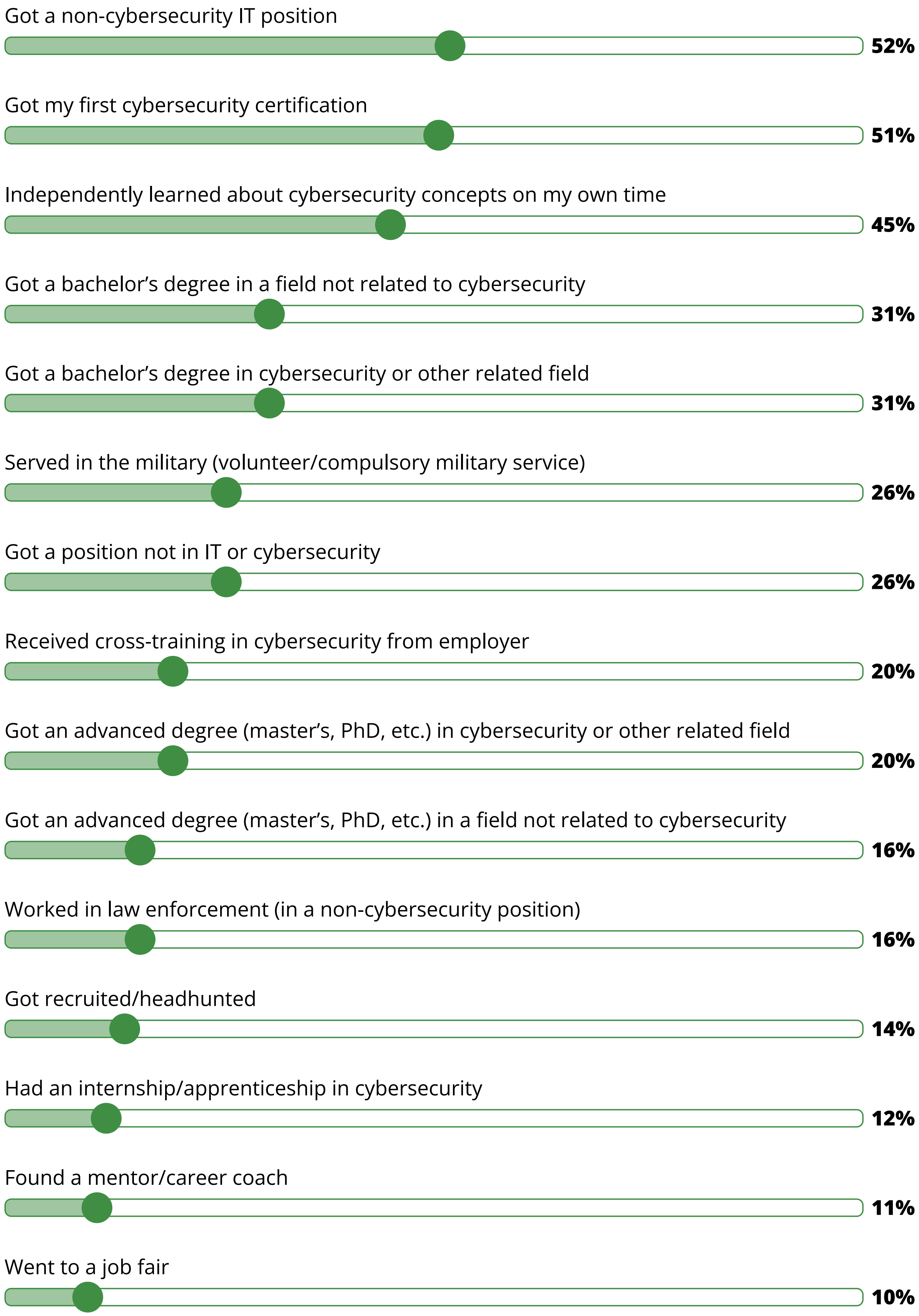
- **For many, IT is a stepping stone into cybersecurity.** 52% of cybersecurity professionals kickstart their careers with a non-cybersecurity IT position. The next most popular pathways into the profession are by earning a cybersecurity certification (51%) or independently learning about cybersecurity concepts outside of formal training (45%). More interestingly, earning a bachelor's degree in cybersecurity (31%) is less popular than all the above as a precursor to joining the profession (see figure 35.)

- **Challenging work and career advancement are key motivators.** After entering the industry, cybersecurity professionals focus on gaining traction in their new roles more than anything else. The most popular next milestones in a cybersecurity career include earning a promotion from a practitioner to a managerial/leadership role (35%), earning a certification for the first time (32%), changing role directions from a specialist to a generalist (26%) or changing back from generalist to specialist (19%). Only 16% report leaving for a new profession, almost the same amount who leave to pursue higher education in cybersecurity or a related field (14%). This showcases the "stickiness" of this career path. After joining the industry, cybersecurity professionals are more motivated to increase responsibility in their current roles and improve their skills for that role, rather than making another career pivot (see figure 36).

FIGURE 35

Which of the following did you do before your first cybersecurity job?

(Showing 15 top ranked responses)

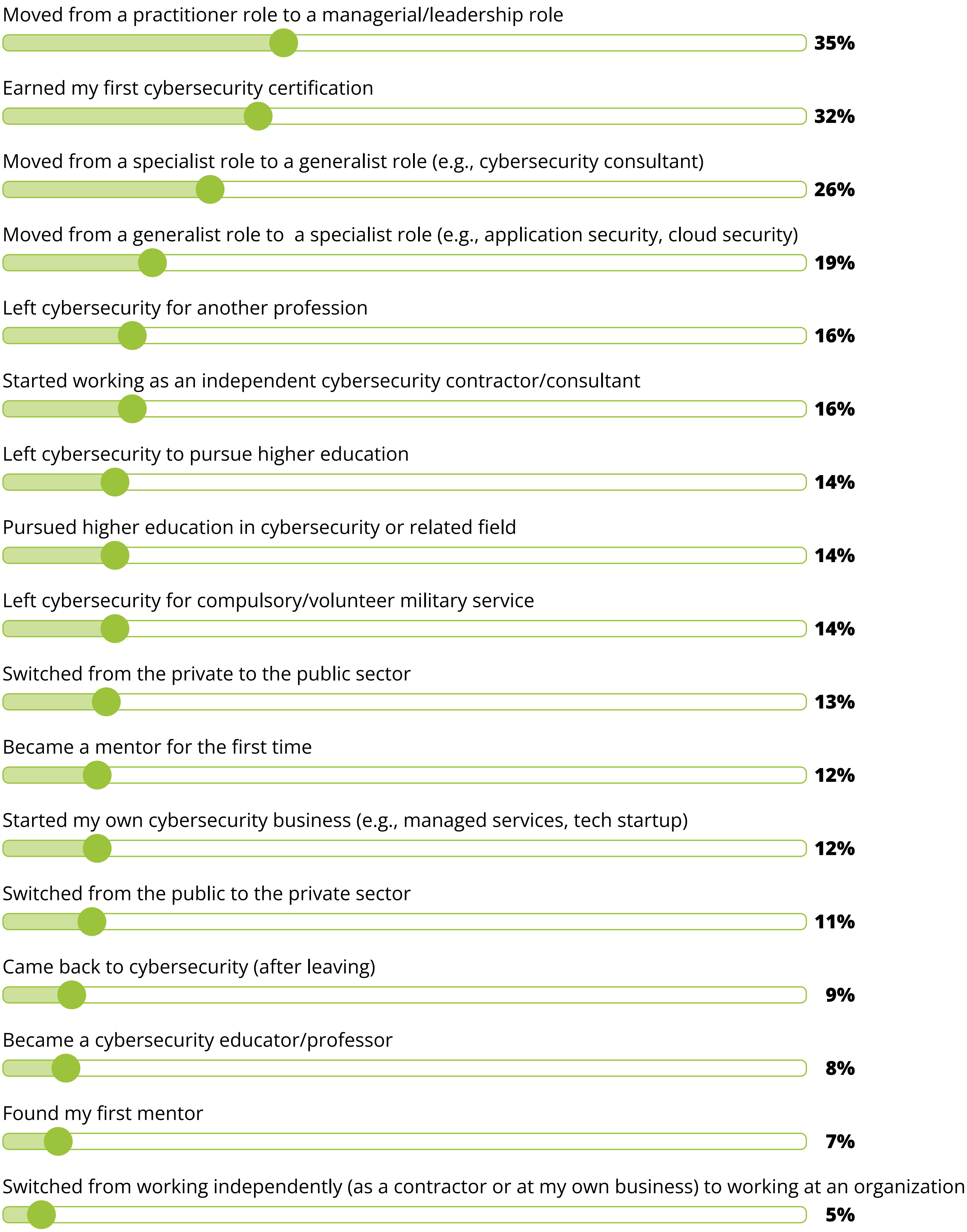


Base: 13,103 global cybersecurity professionals

FIGURE 36

Which of the following did you do after you took your first cybersecurity job?

(Showing top 17 ranked responses)

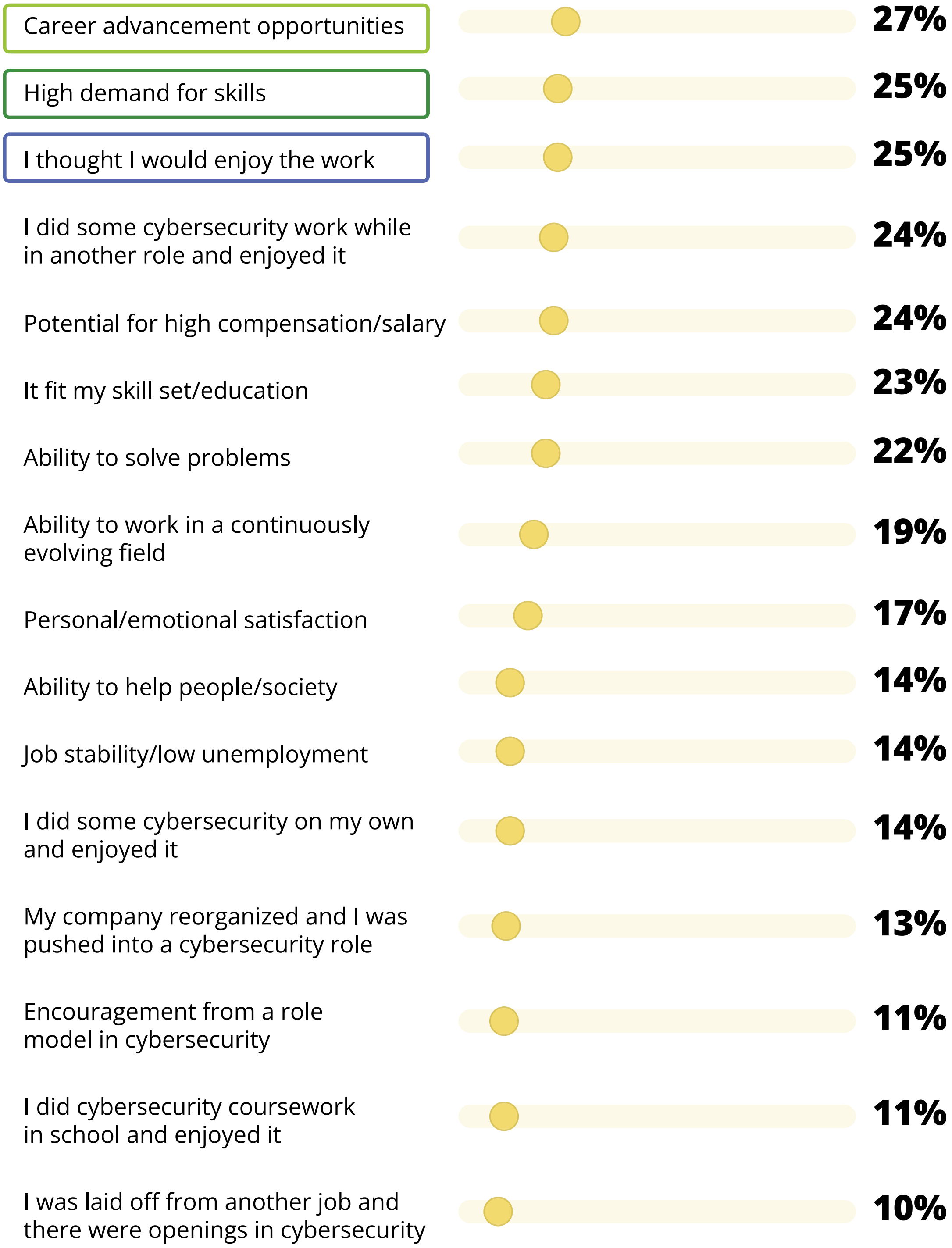


Base: 12,154 global cybersecurity professionals

A number of factors drive the motivation to enter and continue working in the cybersecurity profession, and these can differ based on industry. Primarily, the prospect of career advancement opportunities (27%), skills demand (25%), enjoyment (25%) and high compensation (24%) are attracting people to join and stay in cybersecurity (see figure 37).

FIGURE 37

Which of the following best describes why you originally entered the cybersecurity profession?



Career advancement opportunities

1. **Healthcare (33%)**
2. Government (31%)
3. Aerospace (31%)

High demand for skills

1. **Military (29%)**
2. Aerospace (28%)
3. Food/beverage (28%)

I thought I would enjoy the work

1. **Financial services (29%)**
2. Consulting (28%)
3. Non-security software/ hardware (26%)

Base: 14,865 global cybersecurity professionals

The happiest employees are those who are challenged to continue adapting and evolving — as evidenced by our research finding that employees with the highest EX ratings are most motivated by the ability to work in a continuously evolving field that fits their skill set/education. Conversely, professionals who have been pushed into cybersecurity by their organization or through a layoff at another organization have the lowest EX ratings. Decisions made by professionals who have freedom of choice are the most motivating (see figure 38).

FIGURE 38

Which of the following best describes why you originally entered the cybersecurity profession?

MOTIVATIONS WITH HAPPIEST SECURITY WORKERS

MOTIVATION FOR ENTERING SECURITY	AVERAGE EX RATING
Ability to work in a continuously evolving field	52.98
It fit my skill set/education	52.49
Career advancement opportunities	52.16
Ability to solve problems	52.12
High demand for skills	52.06

MOTIVATIONS WITH LEAST HAPPY SECURITY WORKERS

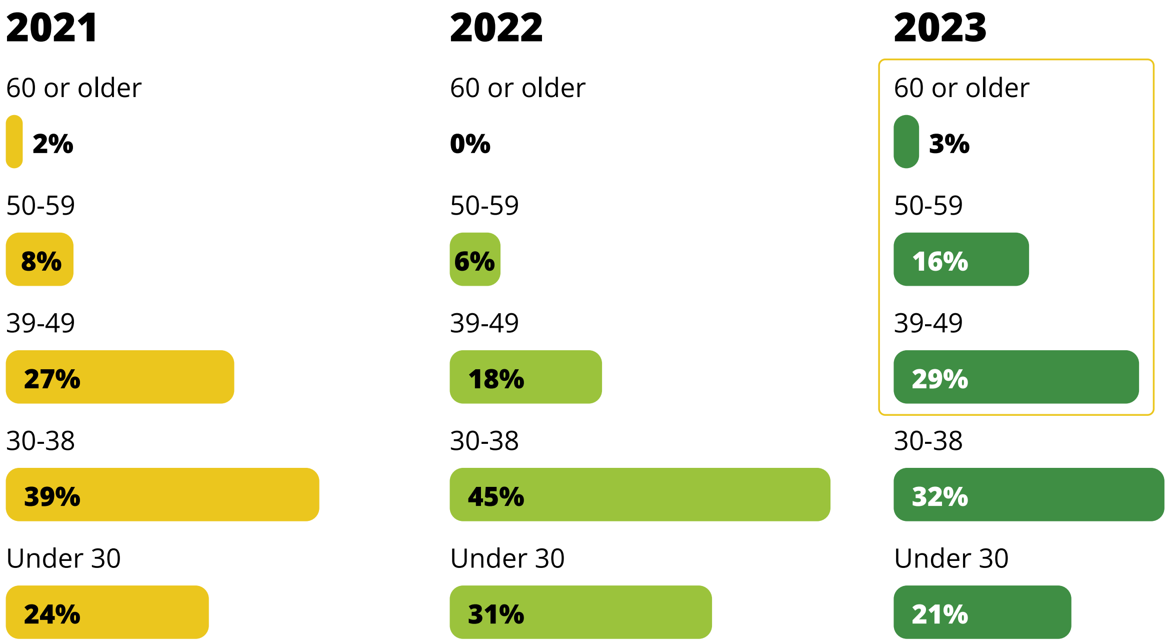
MOTIVATION FOR ENTERING SECURITY	AVERAGE EX RATING
My company reorganized and I was pushed into a cybersecurity role	48.43
I have role models in my life in cybersecurity (e.g., family members, mentors) who encouraged me	48.64
I was laid off from another job and there were openings in cybersecurity	50.54
I did some cybersecurity on my own and enjoyed it	50.63
Job stability/low unemployment	50.79

Base: 14,865 global cybersecurity professionals

- **Pathways are changing.** In 2023, new entrants into the cybersecurity profession are considerably older on average than they have been in the past, with 48% of new entrants joining at age 39 years or older. This is a significant difference from 2022 (24%) and shows a change in the pathways into cybersecurity (see figure 39). Besides the change in age of new cybersecurity professionals, we also see a significant shift in the backgrounds of workers entering the field. New cybersecurity professionals are more likely to have a bachelor's degree in cybersecurity, more likely to come from a non-IT role and less likely to have started in IT (see figure 40).

FIGURE 39

Ages of new entrants into the cybersecurity profession



Base: 695 global cybersecurity professionals who started in the past 12 months; 356 surveyed in 2022 and 610 surveyed in 2021
Note: Total percentages may not equal separate values due to rounding.

FIGURE 40

NEW CYBERSECURITY EMPLOYEES (1 YEAR OR LESS IN THE FIELD)		TENURED CYBERSECURITY EMPLOYEES (10+ YEARS IN THE FIELD)
46%	Got cybersecurity bachelor's degree before entering cybersecurity	32%
55%	Worked in IT before entering cybersecurity	**63%**
39%	Worked in a non-IT role before entering cybersecurity	28%
24%	Had an internship or apprenticeship in cybersecurity before their first job	9%
16%	Influenced to join cybersecurity by role models in their life in the field	9%

Base: 404 new and 6,121 tenured global cybersecurity professionals

Professionals of all ages are united and motivated to join the industry by a simple but powerful feeling — their **sheer enjoyment of the work** (see figure 41). As previously mentioned, career advancement opportunities are the most common motivator to join cybersecurity, but when we look at the age-specific breakdown among workers, we see an interesting trend. Younger professionals (especially those under the age of 30) primarily join the industry based on what they perceive to be an enjoyable career, and older professionals joining midcareer have performed cybersecurity work in another role and decided to join full-time based on their own enjoyment of it.

FIGURE 41

Which of the following best describes why you originally entered the cybersecurity profession?

(Showing top motivating factors)

UNDER 30	30-38	39-49	50-59	60 OR OLDER
I thought I would enjoy the work **27%**	Career advancement opportunities **26%**	Career advancement opportunities **27%**	I did some cybersecurity work while in another role (e.g., general IT) and enjoyed it **30%**	I did some cybersecurity work while in another role (e.g., general IT) and enjoyed it **31%**
Potential for high compensation/ salary **27%**	I thought I would enjoy the work **26%**	High demand for skills **25%**	Career advancement opportunities **28%**	Career advancement opportunities **31%**
Career advancement opportunities **24%**	Potential for high compensation/ salary **25%**	I thought I would enjoy the work **25%**	High demand for skills **25%**	It fit my skill set/education **28%**
High demand for skills **24%**	High demand for skills **25%**	I did some cybersecurity work while in another role (e.g., general IT) and enjoyed it **25%**	It fit my skill set/education **24%**	Ability to solve problems **28%**
Ability to solve problems **24%**	Ability to solve problems **22%**	Potential for high compensation/ salary **24%**	Ability to solve problems **24%**	High demand for skills **26%**

Base: 14,145 global cybersecurity professionals

What It Means for Organizations

New Career Pathways Shape the Future Cybersecurity Workforce

Cybersecurity career paths are shaped by the professionals with traditional and non-traditional experiences who get hired, as well as the organizations that make the decisions to hire them. As more professionals with diverse backgrounds join the industry, new pathways open and evolve the expectations and recruiting habits of hiring managers.

Here are our key takeaways for organizations and professionals with the ability to impact the career pathways for a new generation of cybersecurity professionals:

- **Organizations, rethink your hiring parameters.** New career trajectories and hiring trends make cybersecurity a more attractive place for technically skilled workers of all ages, not just those with traditional education or cybersecurity experience. Organizations seeking to nurture a skilled cybersecurity team should also look for those with non-traditional backgrounds and expand their internal and external recruiting.
- **Professionals, stay agile (and satisfied) by challenging yourselves.** Enjoyment, challenge and career advancement go hand in hand. The happiest employees are those who are challenged to continue adapting and evolving, as evidenced by our EX rating. Cybersecurity is a continuously evolving field, and it’s important to evolve with it. Ask your employer about their professional development opportunities, certifications and skills development programs. This will help you stand out as a key contributor, and help you build new competencies for the future.

Skills in Demand

As with pathways into the field, the demand for new cybersecurity skills is evolving. Cloud computing security continues to be the most desired technical skill set, but the perceived demand for AI/machine learning skills is growing quickly. In addition, the unstable market environment gives rise to a demand for more curious and communicative employees with professional experience. Those with technical on-the-job experience and relevant certifications are more attractive to recruiters than those entering the market with just a degree.

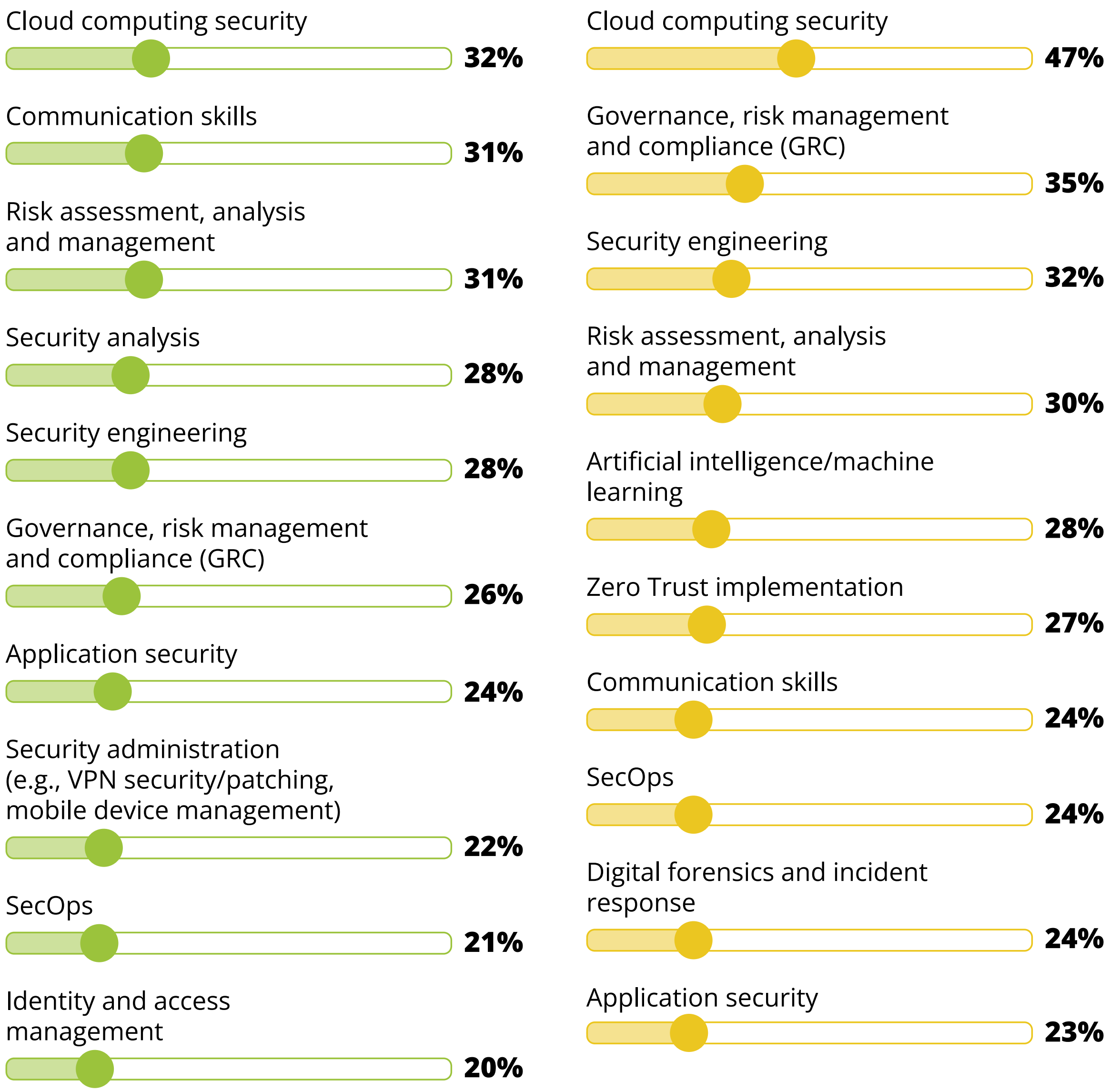
We interviewed both hiring managers and professionals without hiring responsibilities to uncover the most desirable skills, qualifications and experiences that drive recruiting and education demand within the cybersecurity world. Here's what we found:

- **Cloud computing security is a critical skill, but it's in short supply.** Cybersecurity professionals (non-hiring managers) consider cloud computing security to be the most in-demand skill for those looking to advance their careers (47%). Hiring managers continue to validate this perception — for the second year in a row, cloud computing security (32%) is the most desirable skill sought by cybersecurity hiring managers who are looking for recruits. Hiring managers are also prioritizing risk assessment, analysis and management (31%); security analysis (28%); and security engineering (28%) as attractive skills for prospective employees (see figure 42).

  Contributing to the high demand for cloud computing security skills is the aforementioned supply shortage of cybersecurity professionals who have experience in this area. As previously reported, cybersecurity professionals said that cloud computing security is the number one area where there are skills gaps on their team (35%). This only makes the skill more attractive to hiring managers.

- **Demand for AI/ML skills is growing.** Although it's not currently a top requirement from hiring managers, the demand for artificial intelligence skills is growing in the eyes of the average cybersecurity professional. AI/ML skills (28%) are among the top five categories for in-demand skills (see figure 43). As recent as our 2022 study, AI/ML did not even make the top ten for most in-demand skills and was ranked close to the bottom. In the coming years, this skill has the potential to spike in demand as AI matures and influences various aspects of cybersecurity threats and defense.

FIGURE 42



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

(Showing top ten responses)

ASKED TO HIRING MANAGERS

Which of these skills do you think are most in demand for security professionals looking to advance their careers (via new jobs and promotions)?

(Showing top ten responses)

ASKED TO NON-HIRING MANAGERS

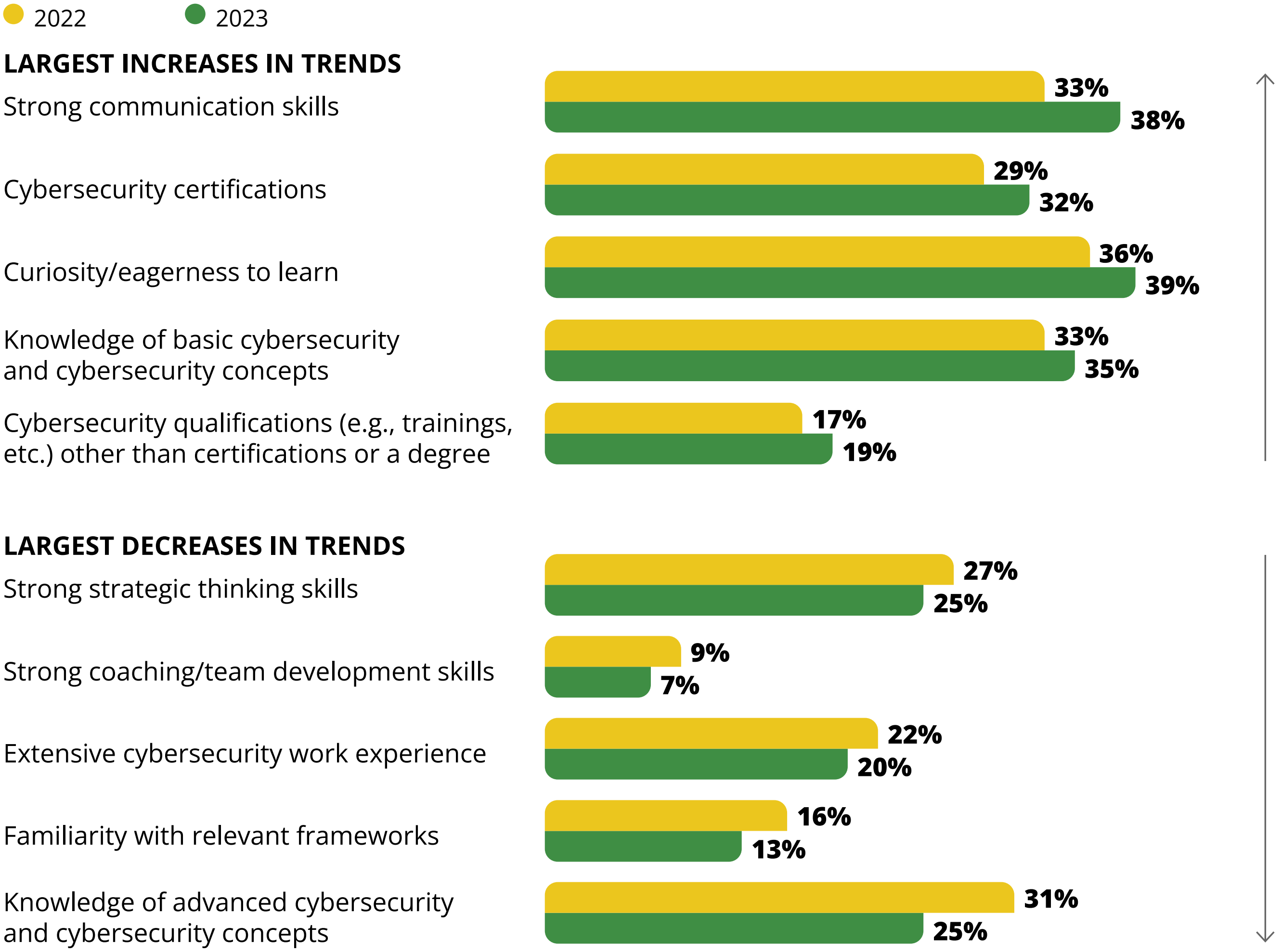
Base: 7,143-7,184 global cybersecurity professionals
Note: "Don't know/does not apply" responses were removed from the sample base.

- **Curiosity, communication and certifications are growing in importance.** Cybersecurity professionals consider problem-solving abilities to be the most important qualifying characteristic for themselves on the job (45%). However, curiosity/eagerness to learn (39%), communication skills (38%) and cybersecurity certifications (32%) have grown in value year over year. When compared to 2022, these traits increased in importance by 3% to 5%, and this upward trend reflects the needs of the modern risk landscape. When operating in a market characterized by instability, organizations need professionals who are knowledgeable, adaptable and efficient facilitators of information (see figure 43).

FIGURE 43

What are the top five most important qualifications for cybersecurity professionals seeking employment?

(Showing top five and bottom five responses)



Base: 14,865 global cybersecurity professionals

- **Professional experience and certifications are seen as more valuable than formal education.** Cybersecurity skills are shaped by education, training and experience. When asked about the experiences and education that constitute the ideal cybersecurity candidate, respondents made it clear that experience and certification top all else. Senior-level cybersecurity experience (86%) was highly favored over advanced doctoral degrees (14%) (see figure 44).

  Experience carries weight, even if it isn't specific to cybersecurity. Mid-level non-cybersecurity technical experience (63%) was favored over entry-level cybersecurity experience (37%). However, entry-level cybersecurity experience (70%) is still more important than entry-level cybersecurity education (30%). **This tells us that cybersecurity professionals view professional exposure in any manner as more valuable than education in a classroom or virtual setting.**

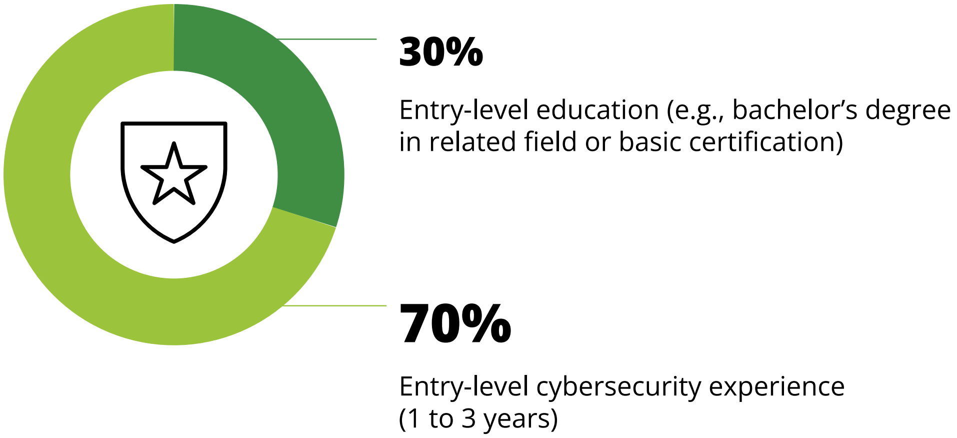
  Certifications are also a highly regarded form of cybersecurity qualification. They are favored over both a bachelor's degree in a related field (66% vs. 34%) and independent competition experience (54% vs. 46%) (e.g., hackathons). Despite the new pathways and trends shaping the modern cybersecurity profession, certifications continue to be a core ingredient for the ideal cybersecurity candidate.

FIGURE 44

If you were to design your ideal cybersecurity candidate, which of these things would you prefer?

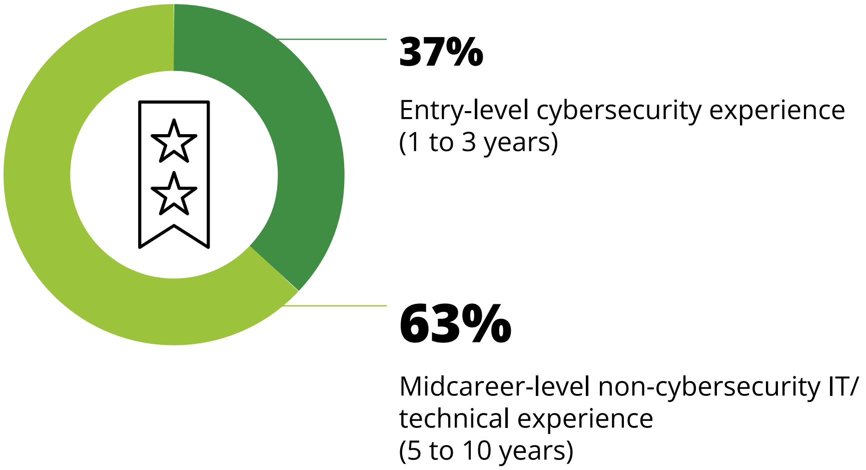
Entry-level cybersecurity experience is preferred to entry-level degrees

Base: 13,742



Mid-level (non-cyber) experience is preferred to entry-level cyber experience

Base: 13,615



Senior-level cybersecurity experience is perceived as far more valuable than advanced degrees

Base: 13,500

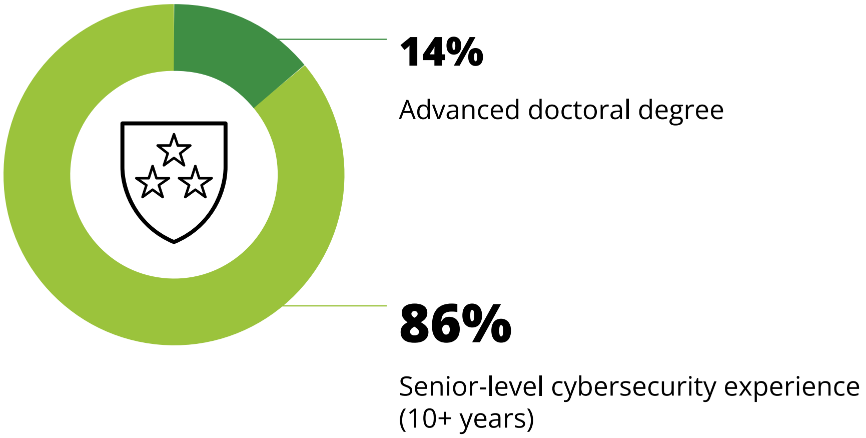
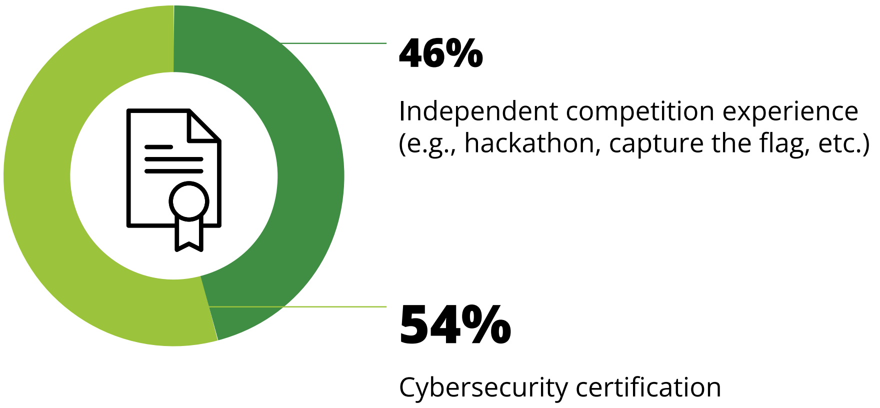


FIGURE 44

If you were to design your ideal cybersecurity candidate, which of these things would you prefer?

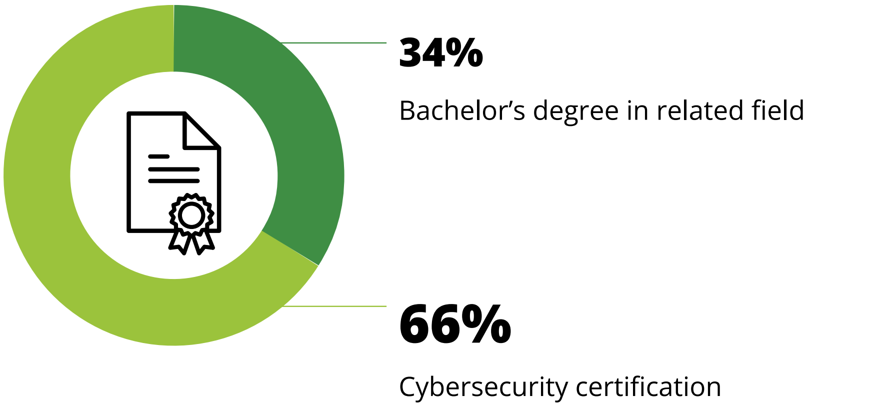
Certifications are more valuable than independent experience

Base: 13,222



Certifications are more valuable than entry-level degrees

Base: 13,496



Base: 13,222-13,742 global cybersecurity professionals
Note: "Don't know/does not apply" responses were removed from the sample base.

What It Means for Organizations

Continue to Nurture and Develop Skill Sets for Well-Rounded Talent

The current macroeconomic environment calls for a generation of cybersecurity workers who are curious, agile and open to new challenges. This is who modern organizations seek as they grapple with cutbacks and skills gaps.

Here are our key takeaways for organizations and professionals looking to hire, nurture and develop skill sets to fill gaps and improve the future of work:

- **Organizations, expand basic cybersecurity training to everyone.** For many organizations, the need for basic cybersecurity skills has eclipsed the need for niche and advanced skill sets. Attributes like eagerness to learn, communication skills and curiosity have never been more important. To create more well-rounded and knowledgeable cybersecurity employees, try offering basic training/professional development to other departments within the organization. Encouraging basic skills development on a holistic level can also organically promote your cybersecurity team as a new career pathway.

- **Professionals, supplement education with hands-on experience.** Cybersecurity professionals (especially hiring managers) favor on-the-job experience over traditional education, and this includes non-cybersecurity experience. So those pursuing a career in cybersecurity should try to supplement their education with hands-on, technical on-the-job experience — whether an internship, certification or independent competition (hackathon, etc.) — to diversify their resume.

Certifications

Certifications continue to be a pillar of cybersecurity professional development. Certification activity and planning have stayed generally constant, which shows that professionals remain steadfast in their journey to expand their cybersecurity skills and knowledge.

Both employees and their organizations have expressed resilience and dedication to certifications in an uncertain economy. Even amid corporate cutbacks like hiring freezes and job layoffs, more than half of professionals are offered reimbursements for certification exams by their employer. Employers that do so are successful at filling skills gaps.

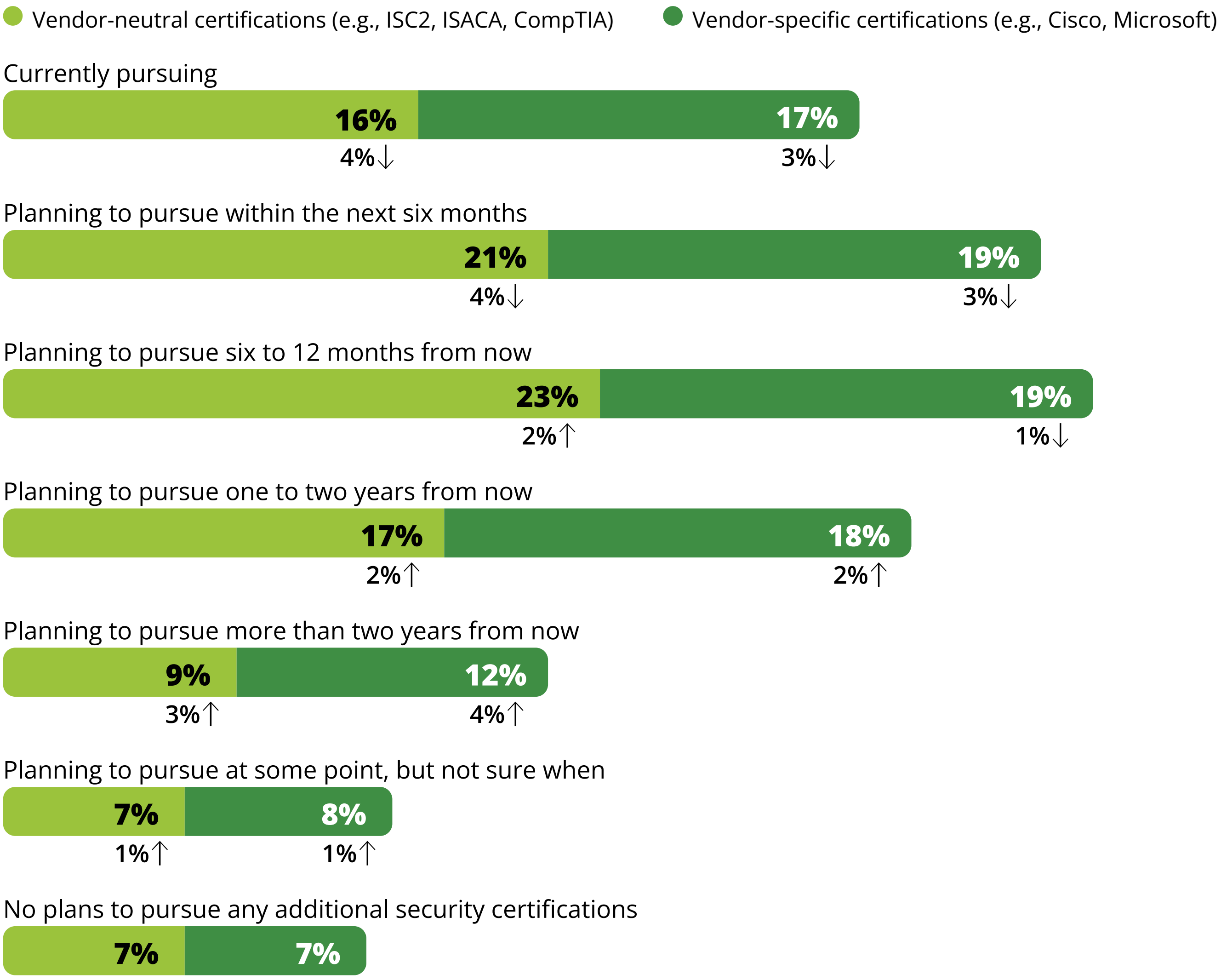
We spoke to more than 14,000 cybersecurity professionals to learn about how and when they plan to earn certifications and found that:

- **Certification pursuit remains strong.** Cybersecurity professionals continue to plan ahead for their professional development, with only minor postponements from near-term to long-term plans. Within the next six months, 21% of respondents plan to pursue a vendor-neutral certification, with 49% thinking longer-term (six months to two years and beyond). Those planning for vendor-specific certifications are behaving similarly, with 19% planning for the immediate future and 49% extending their pathway beyond six months. On average, we observed a 6% increase in those who are planning on continuing their certification work in the period beyond the next six months. In general, however, the market has not deterred cybersecurity professionals from furthering their education and skill sets (see figure 45).

More than half of cybersecurity professionals receive incentives in the form of certification exam reimbursements (54%).

FIGURE 45

Which of the following best describes your plans to pursue any vendor-neutral or vendor-specific cybersecurity certifications in the future?



Base: 3,818-3,829 global cybersecurity professionals (Panel respondents)
Note: "Don't know/does not apply" responses were removed from the sample base.

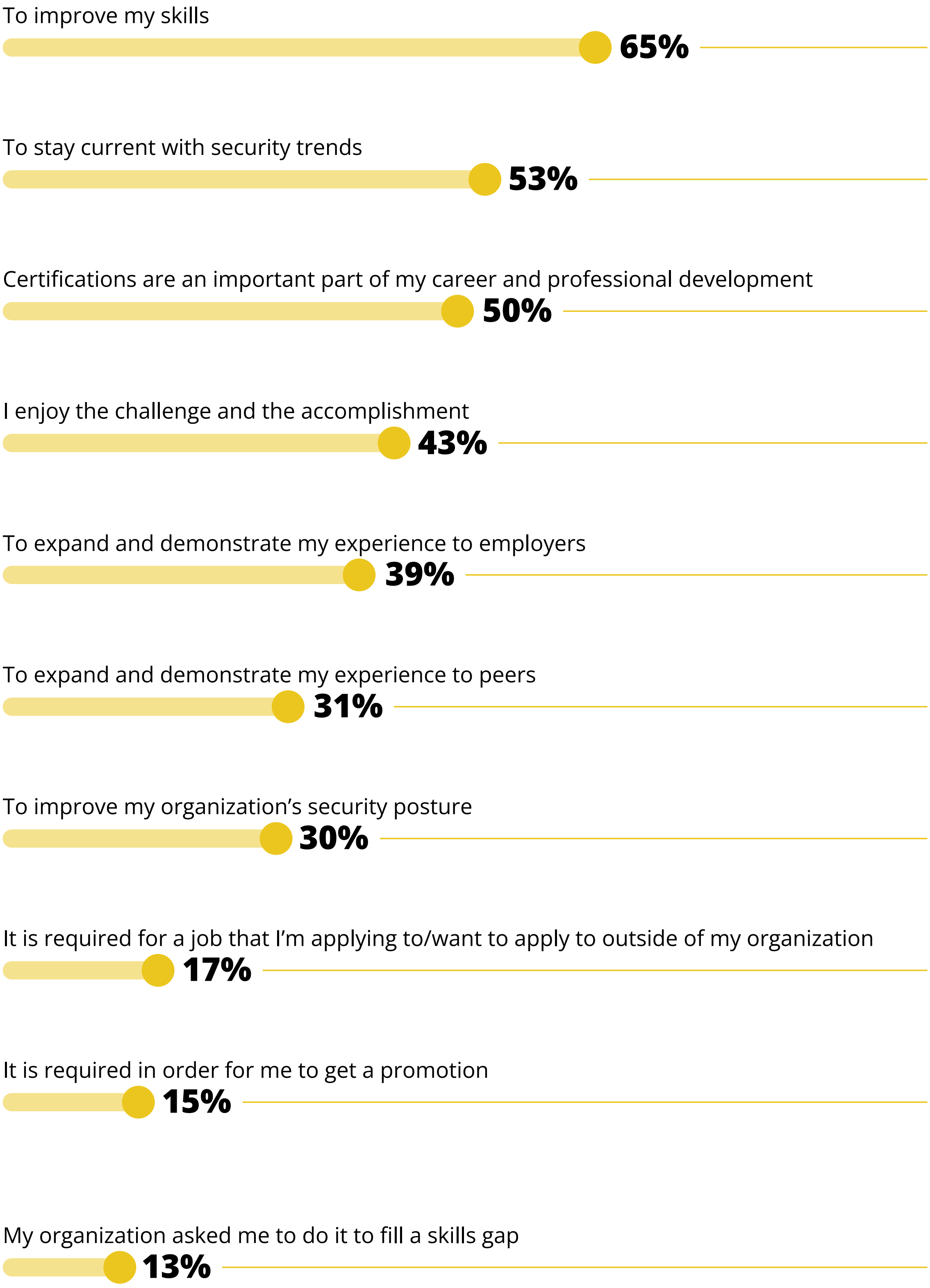
- **Skills growth continues to be the driving motivator for certification.** Cybersecurity professionals are still pursuing certifications to grow and develop their skills (65%). This is true for workers of all ages. Professionals in the 50+ age range (67%) agree to this, and so do those under 49 (65%). This paints a picture of the wide applicability of certifications, regardless of experience or industry tenure.

  Other motivators include staying current with security trends (53%) and the sheer enjoyment of the challenge (43%) (see figure 46). Those with high school diplomas agree more with this (47%) than those with more advanced degrees (42%). Professionals without undergraduate or graduate degrees use certifications to demonstrate their cybersecurity knowledge, skills and abilities.

  While personal motivation is key to earning certifications and growing skills, organizations need to support their employees' pursuit to holistically close skills gaps.

FIGURE 46

You indicated you have plans to get a certification in the future. What is your motivation for doing so?

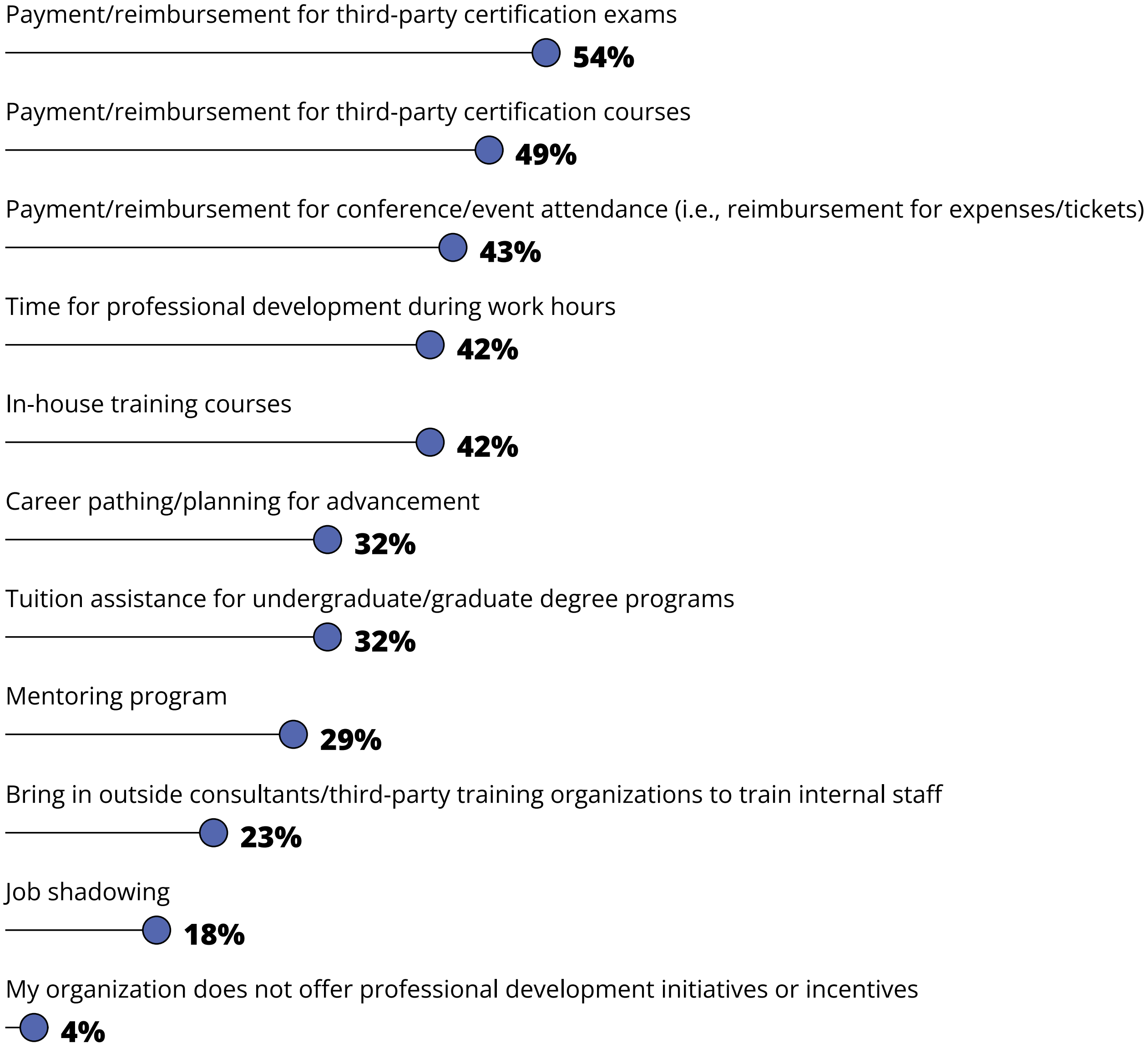


Base: 11,660 global cybersecurity professionals
Note: “Don’t know/does not apply” responses were removed from the sample base.

- **Organizations continue to subsidize certifications as professional development.** Despite economic headwinds, 96% of respondents are offered professional development incentives from their organizations. More than half of cybersecurity professionals receive these incentives in the form of certification exam reimbursements (54%), which continues to be the top mode of educational assistance year over year. Certification reimbursements aren’t the only form of professional development incentive, however. Companies also include reimbursements for conferences/events (43%), in-house training (42%), career pathing/planning for advancement (32%) and tuition assistance (32%) (see figure 47).

FIGURE 47

Which of the following does your organization offer in terms of professional development initiatives/incentives?



Base: 14,009 global cybersecurity professionals
Note: “Don’t know/does not apply” responses were removed from the sample base.

- **Certification reimbursement can shrink skills gaps.** Professional development incentives could be a not-so-secret weapon in the fight against the global cybersecurity gap. 47% of organizations that do not offer reimbursements for certification courses or exams have significant skills gaps in cybersecurity, compared to only 38% that do offer reimbursements. If more organizations encouraged certifications, this could organically nurture core cybersecurity skills without requiring more outside hiring.

  Employees are taking action to fill these gaps. 56% of cybersecurity professionals at organizations with critical skills gaps plan to get a vendor-neutral certification within the next year.

Regions with organizations offering payment/reimbursement for third-party certification exams

North America	62%	Europe	52%
Asia-Pacific	48%	Middle East/Africa	35%
Latin America	33%		

Industries with organizations offering payment/reimbursement for third-party certification exams

Consulting	67%	Financial services	63%
Automotive	40%	Construction	36%

What It Means for Organizations

Expand Your Definition of Professional Development

Certifications are a foundational aspect of skills development, and organizations play a crucial role in making them accessible and available to their employees, especially in an uncertain economic environment. To encourage development from within and close skills gaps, organizations need to ensure their employees know that they are serious about their certification development — enough to dedicate time for them to focus on it.

Here is a key takeaway for companies that want to show their dedication to employees' professional development:

- **Organizations need more than just money to promote skills growth.** Even amid corporate cutbacks like hiring freezes and layoffs, more than half of professionals are still offered reimbursements for certification exams by their organizations. This is an important step toward encouraging skills development, but to truly signal to your employees that you care about their growth, you need to give them time to earn it. Reserving specific blocks of study time for certification or professional development seminars on a biweekly or even monthly basis will help to signal to your employees that you care about their skills growth. It will also provide breathing room for employees who feel overworked or those without the ability to dedicate time outside their workday to focus on training rather than emails or personal responsibilities.

Cybersecurity Landscape: Present & Future

Three out of four cybersecurity professionals view the current landscape as the most challenging it's been in the past five years. The modern economic environment has increased the risk of malicious insiders, and staff/skill shortages impede the ability of cybersecurity teams to properly secure their organizations. As professionals adapt to today's challenges, they are also looking to the horizon for emerging threats and opportunities.

The topic of AI is unavoidable in a conversation about the positive and negative impacts of tomorrow's technology. Speculation about its use commands global attention: Will it become a tool for more efficient threat response or a door to more sophisticated attacks? Cybersecurity professionals are weighing these potential futures with cautious optimism to understand and adopt the emerging technology while at the same time preparing for the potential risks that it could create.

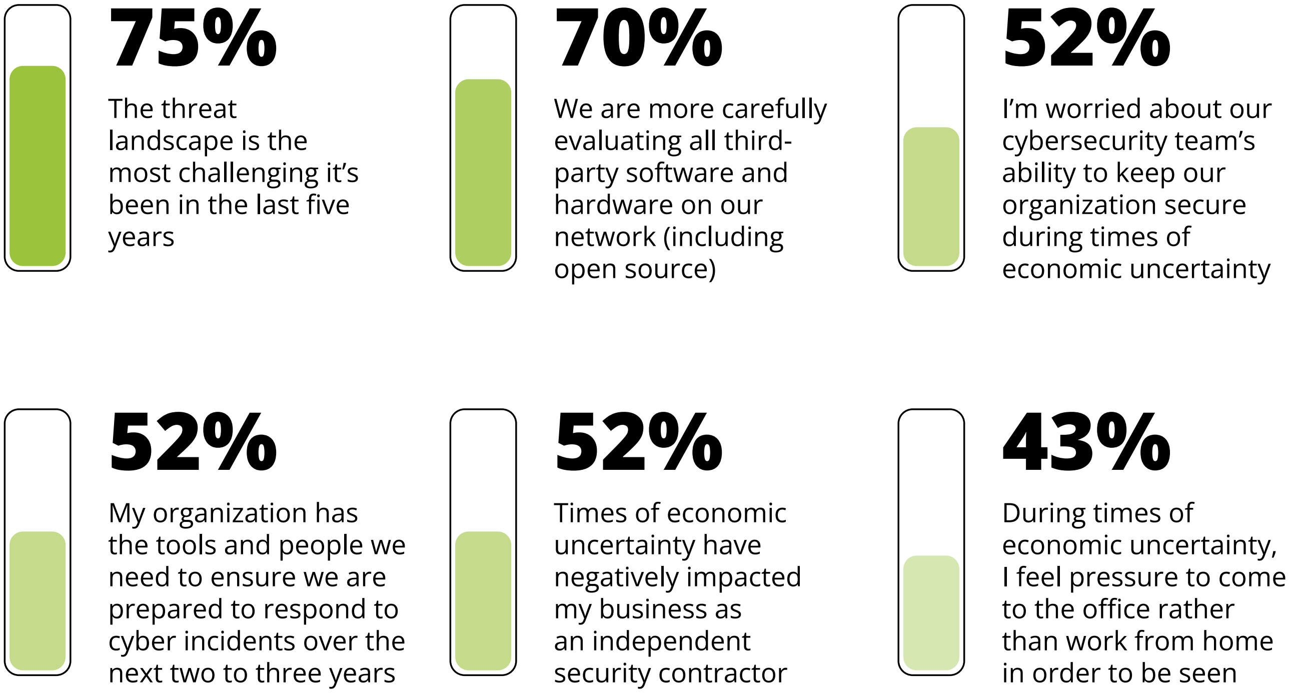
Here is what we learned from cybersecurity professionals who are adapting to today's challenges while preparing for the future of work:

- **For most, the threat landscape has reached a peak**. 75% of all respondents view the current threat landscape as the most challenging it's been in the past five years (see figure 48), and this varies by industry. Respondents from some industries indicated more sensitivity than others to the modern environment: those in healthcare (79%), military (79%), energy/power/utilities (79%), government (78%) and manufacturing (77%) industries agree/strongly agree that they have reached their peak threat level since 2018. Even those that are less sensitive like automotive (64%), construction (65%) and telecom (69%) still mostly agree with this sentiment (see figure 49).

FIGURE 48

How strongly do you agree with the following statements related to the state of cybersecurity work?

(Showing Agree/Strongly Agree responses)



75%
The threat landscape is the most challenging it's been in the last five years

70%
We are more carefully evaluating all third-party software and hardware on our network (including open source)

52%
I'm worried about our cybersecurity team's ability to keep our organization secure during times of economic uncertainty

52%
My organization has the tools and people we need to ensure we are prepared to respond to cyber incidents over the next two to three years

52%
Times of economic uncertainty have negatively impacted my business as an independent security contractor

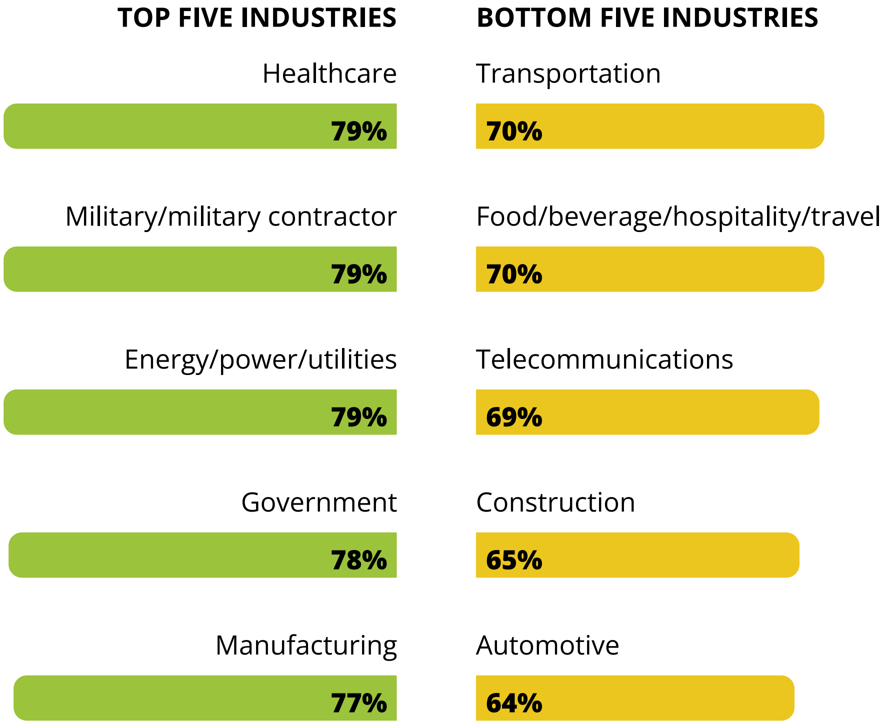
43%
During times of economic uncertainty, I feel pressure to come to the office rather than work from home in order to be seen

Base: 13,048-14,093 global cybersecurity professionals
Note: "Don't know/does not apply" responses were removed from the sample base.

FIGURE 49

The threat landscape is the most challenging it's been in the past five years.

(Showing Agree/Strongly Agree responses)



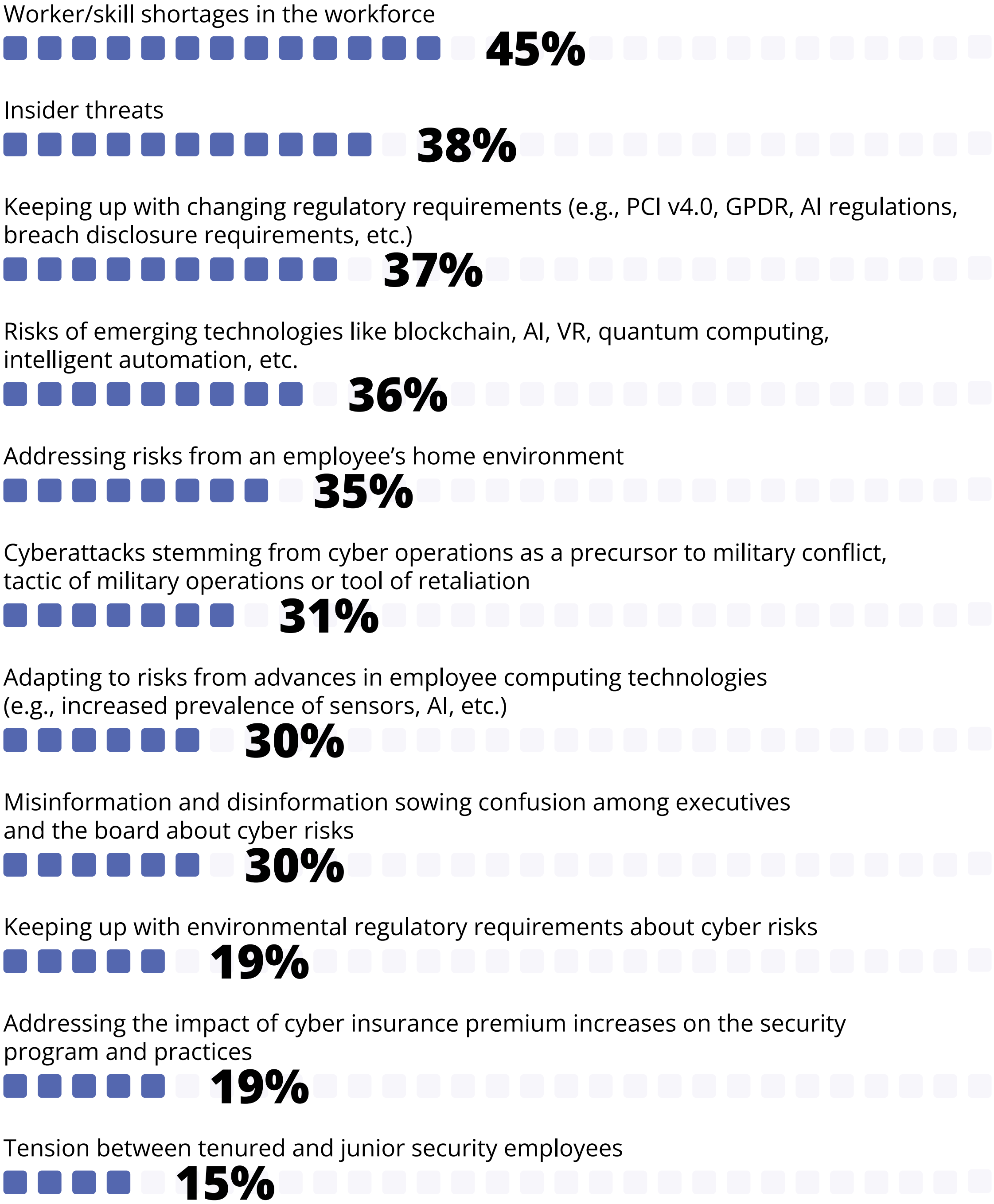
Base: 130-1,239 global cybersecurity professionals in listed industries
Note: "Don't know/does not apply" responses were removed from the sample base.

Contextualizing the modern threat landscape is key to understanding how to prepare for it. Ultimately, only 52% of cybersecurity professionals say that their organization has the tools and people to ensure that they are prepared to respond to cyber incidents over the next two to three years. The same proportion say that they worry about keeping their organization secure during times of economic uncertainty. This uncertainty is more significant among companies who have had cybersecurity layoffs in the past 12 months (63%) versus those who haven't had any layoffs (47%), which prompts the question of whether the security risks of cybersecurity layoffs are worth the cost savings.

- **Staff and skill shortages have shaped the current threat landscape.** In the past 12 months, worker/skills shortages (45%) have been the number one challenge faced by cybersecurity professionals (see figure 50). Geography is a key differentiator here, as respondents in North America (55%) have felt a more significant impact from these shortages than those in other parts of the world like Europe (42%), the Middle East and Africa (42%), Latin America (32%) and Asia-Pacific (31%). This contextualizes the roughly 20% workforce gap increase within North America.

FIGURE 50

What were the biggest challenges cybersecurity professionals faced in the past 12 months?

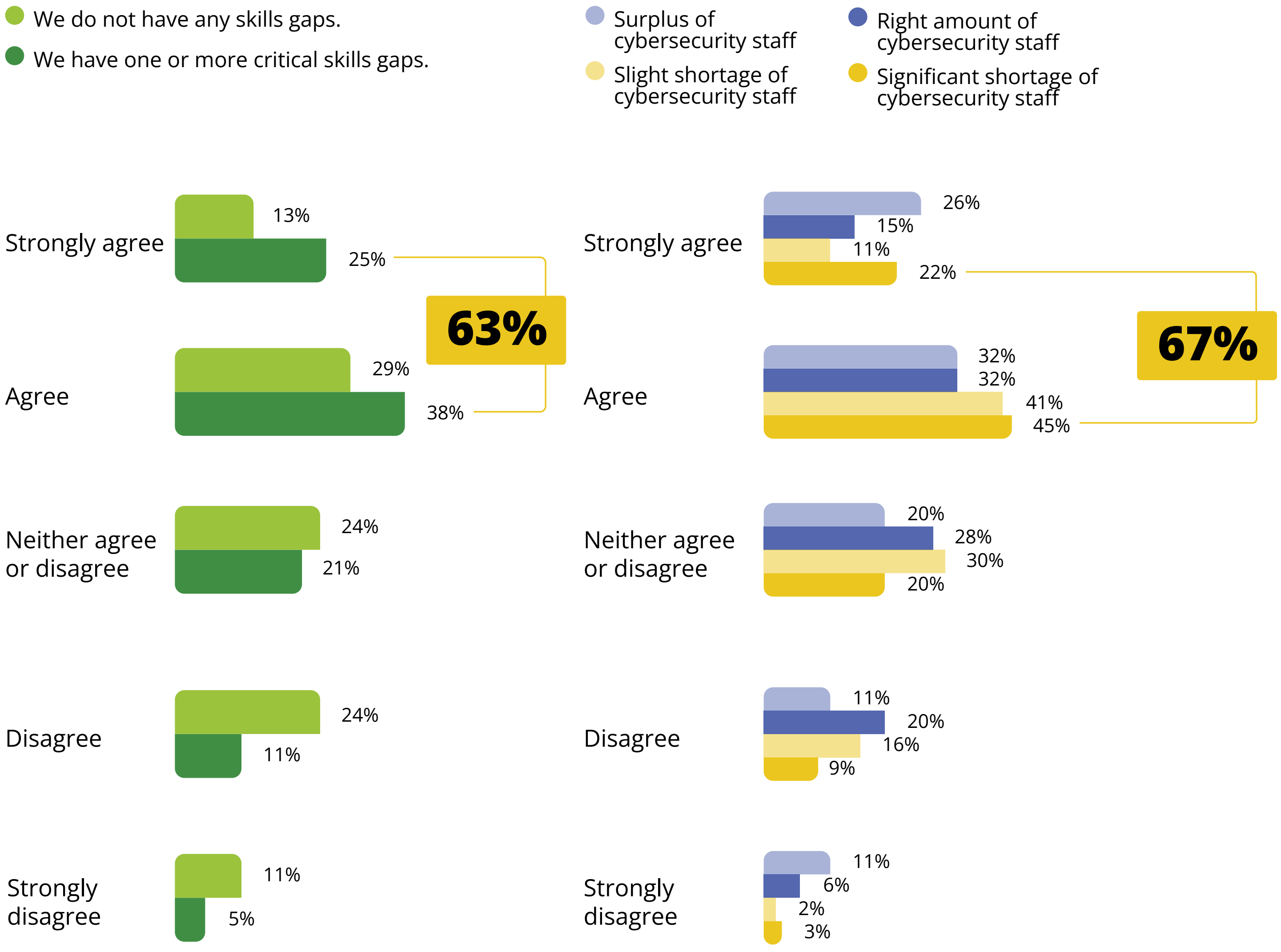


Base: 14,865 global cybersecurity professionals

Two-thirds of respondents from organizations with significant staff shortages (67%) say they worry about their team's ability to keep their organization secure, and 63% of those with skills gaps agree with the same sentiment (see figure 51). In general, 62% of cybersecurity professionals say that corporate cutbacks like layoffs, budget cuts and hiring freezes reduce their ability to prepare for future threats.

FIGURE 51

I’m worried about our cybersecurity team’s ability to keep our organization secure during times of economic uncertainty.



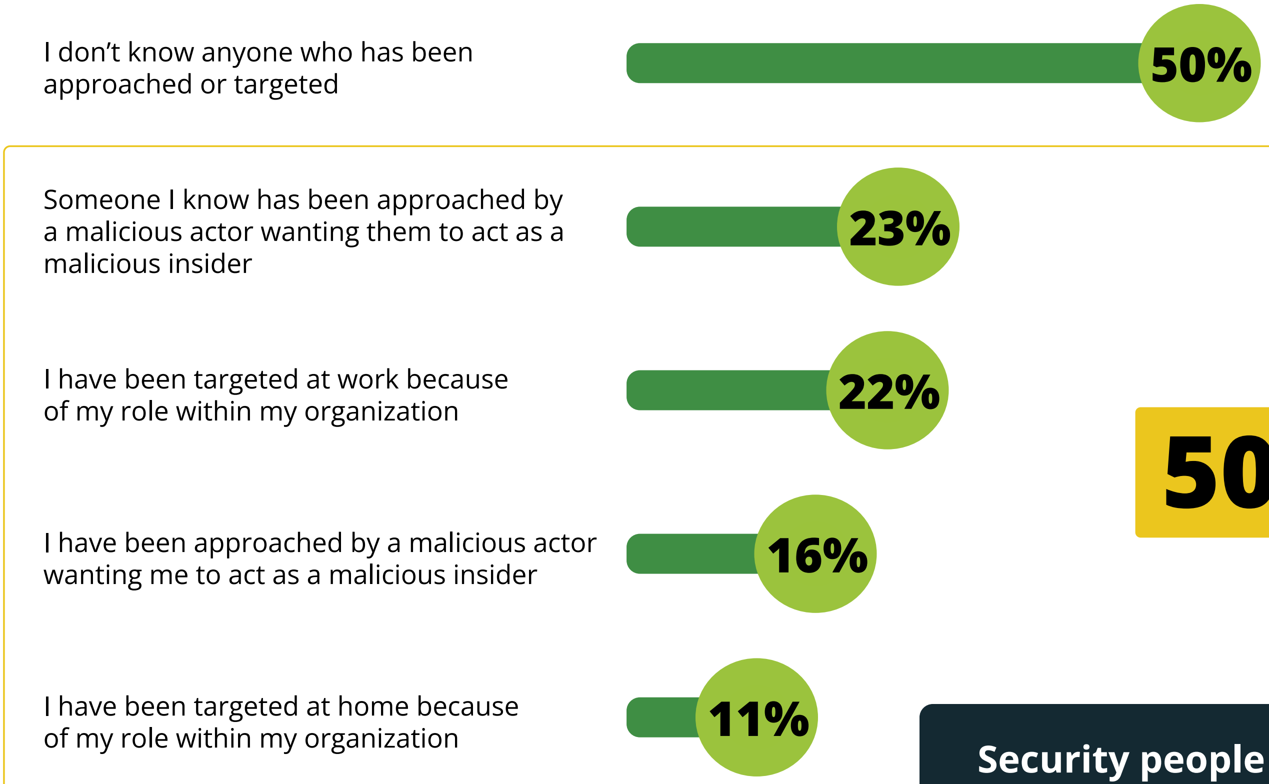
Base: 7,861-11,915 global cybersecurity professionals
Note: Total percentages may not equal separate values due to rounding.

To future-proof themselves from new threats on the horizon, more organizations need to encourage and incentivize skills growth from within through certification programs.

- **Malicious insiders are on the rise.** 71% of respondents agree that times of economic uncertainty increase the risk of malicious insiders, which next to staff/ skill shortages were ranked the second biggest challenge (38%) for cybersecurity professionals in the near term. Even more significant: Half of all cybersecurity professionals taking part in this study have had personal or secondhand contact with a malicious insider within the past year (see figure 52).

FIGURE 52

In the past year, which of the following threat scenarios have occurred?



50%

Security people at orgs that have had security layoffs are 3x more likely to have been approached to act as a malicious insider.

Base: 14,865 global cybersecurity professionals

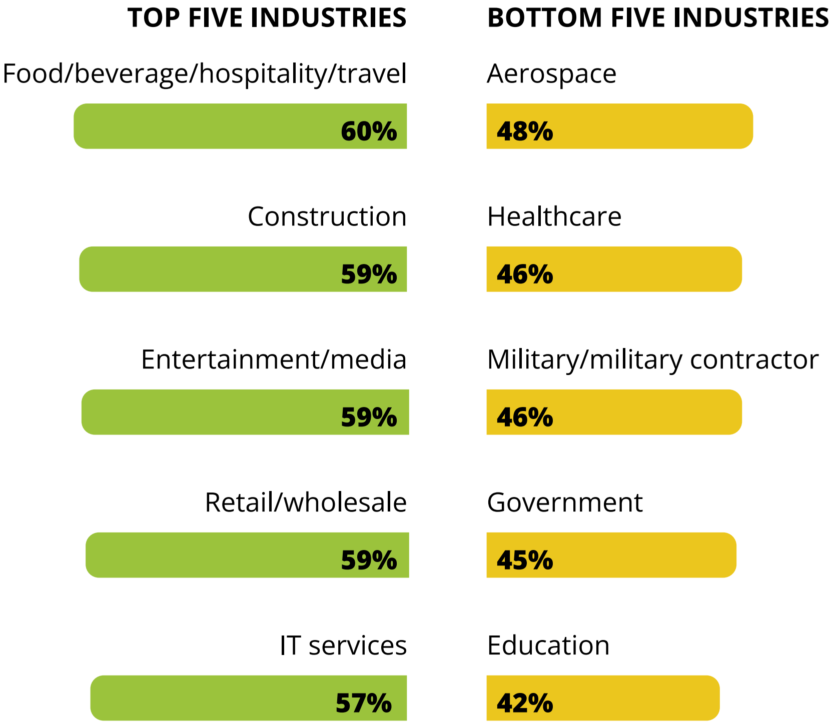
Cybersecurity professionals at organizations that have had layoffs in cybersecurity are three times more likely to have been approached to act as malicious insiders. It remains to be seen whether the future of work and the impact of emerging technologies have a positive or negative impact on this trend.

- **Service and manufacturing organizations are better prepared than federally funded entities for future risk.** Cybersecurity professionals working for a diverse cross-section of industries around the world shared how well-prepared their organizations are for what the future holds. Most respondents working in the food/ hospitality/travel (60%), construction (59%), entertainment/media (59%), retail/ wholesale (59%) and IT services (57%) industries are confident in their ability to manage cybersecurity risk in the next two to three years. **This confidence contrasts with government-led and publicly funded institutions like education (42%), government (45%), military/military contracting (46%), healthcare (46%) and aerospace (48%) — less than half of whom believe they can withstand future cyber incidents (see figure 53).**

FIGURE 53

My organization has the tools and people we need to ensure we are prepared to respond to cyber incidents over the next two to three years.

(Showing Agree/Strongly Agree responses)

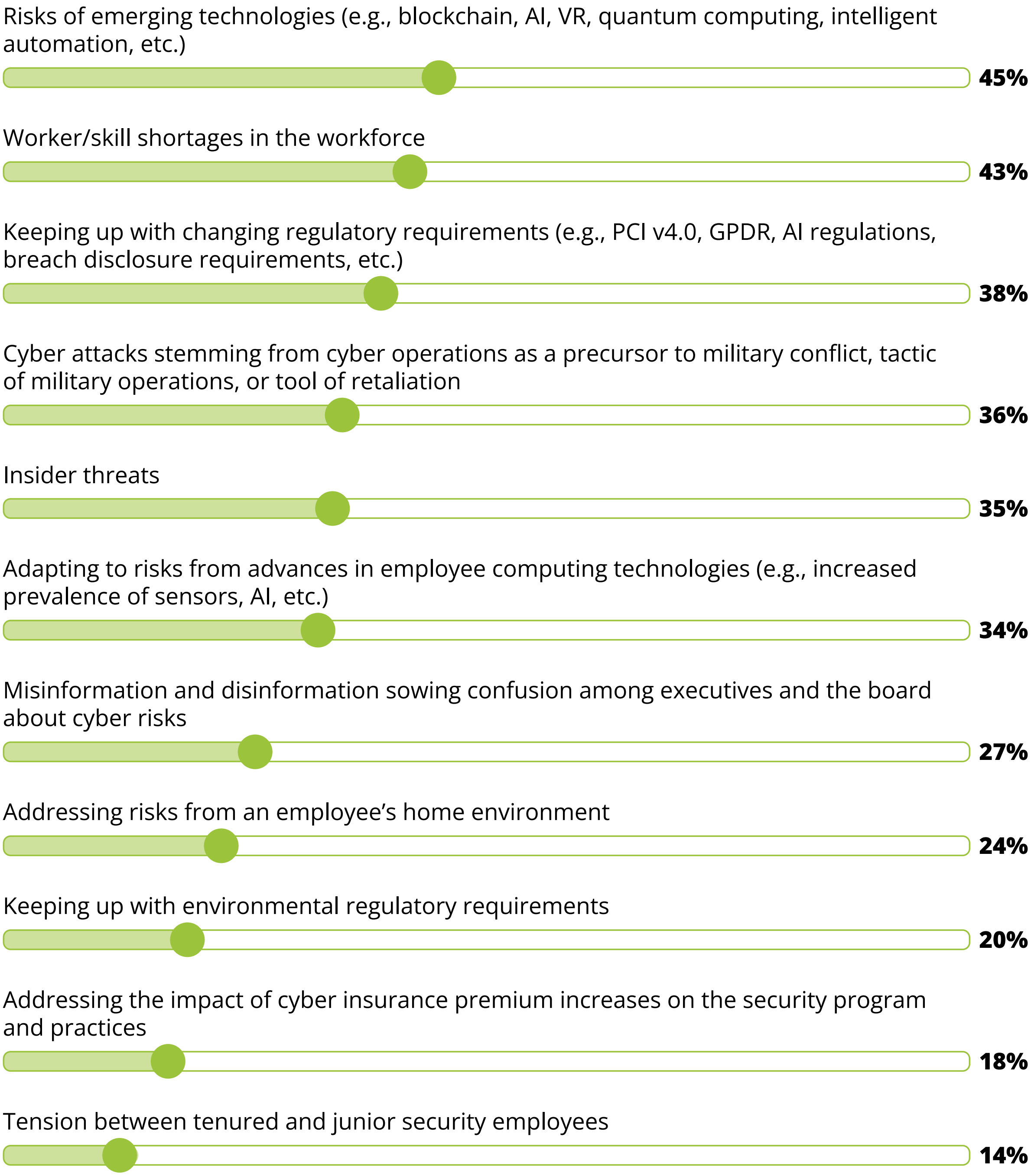


Base: 129-1,210 global cybersecurity professionals in listed industries.
Note: "Don't know/does not apply" responses were removed from the sample base

- **Cybersecurity professionals approach AI with cautious optimism.** Within the next two years, roughly half (45%) of cybersecurity professionals surveyed believe that AI will overtake worker/skill shortages to become the biggest challenge faced by the industry (see figure 54).

FIGURE 54

What are the biggest challenges that cybersecurity professionals will have to face over the next two years?

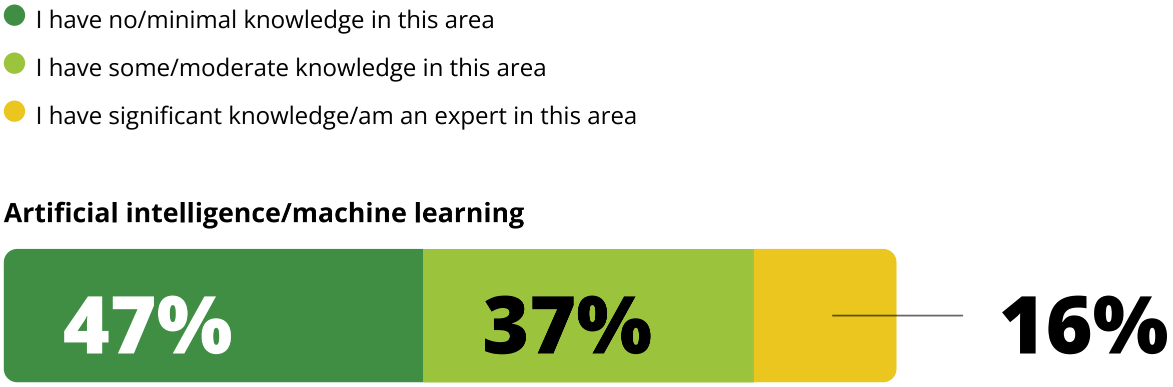


Base: 14,865 global cybersecurity professionals
Note: Showing top five ranked

As AI/ML gains prominence, we have learned that employees are much less prepared to wield and effectively use its power compared with other cybersecurity competencies. 84% of respondents say that they have no/minimal knowledge or only some/moderate knowledge of AI/ML (see figure 55). The gap in AI/ML skills (32%) is second only to the gap in cloud computing security (35%), and based on the year-over-year rise in demand for these skills among cybersecurity employees, access to more AI-based professional development is needed immediately.

FIGURE 55

What is your level of expertise in each of the following areas/skills?

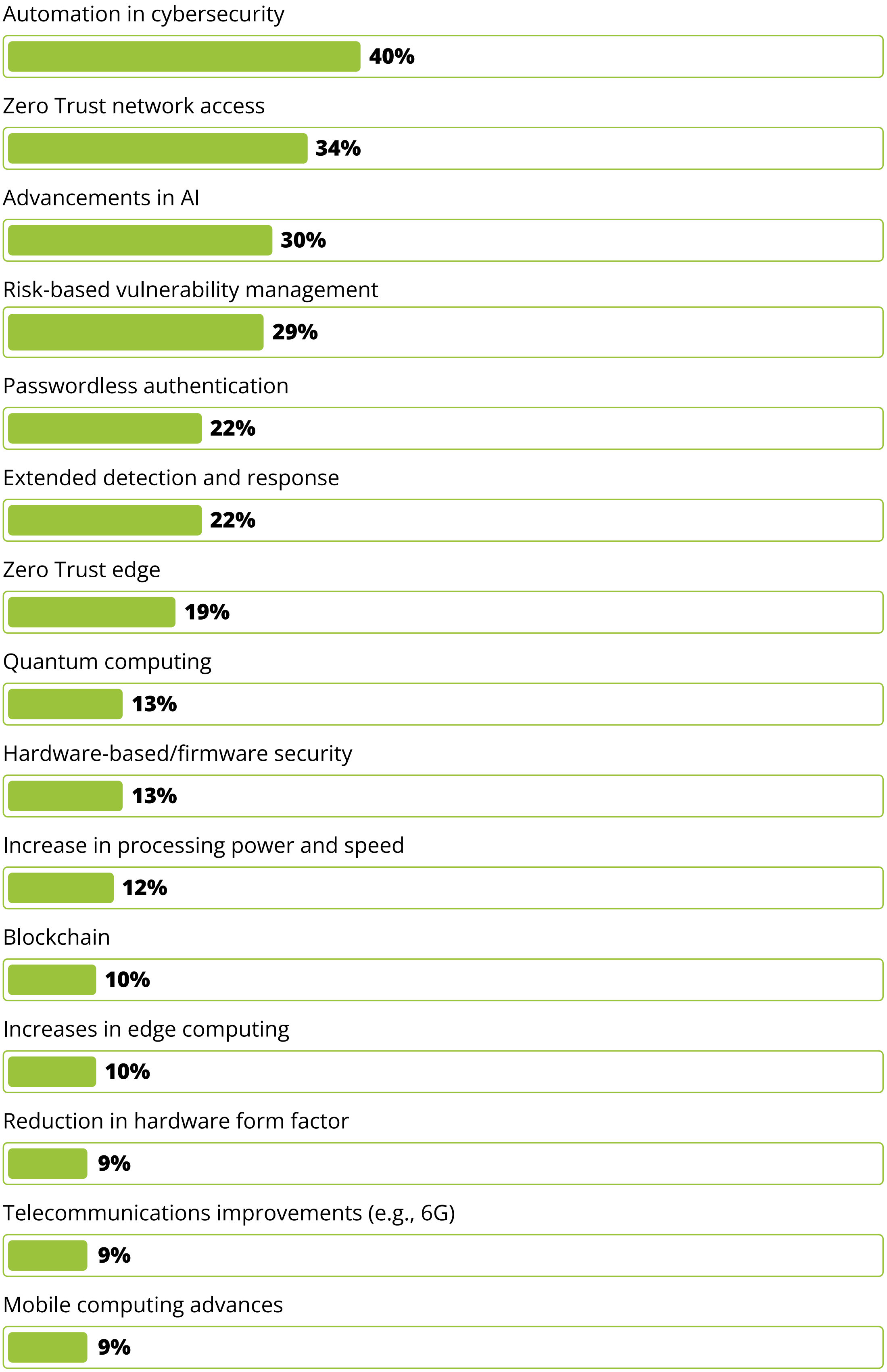


Base: 14,297 global cybersecurity professionals. “Don’t know/does not apply” responses were removed from the sample base

Nevertheless, many cybersecurity professionals are optimistic about the prospects of AI. Respondents believe that advancements in AI will have one of the top three most positive impacts on their ability to secure their organization (30%), behind Zero Trust (34%) and automation (40%) (see figure 56). Anticipating the need to better understand AI, organizations are taking action to regulate it. 52% of cybersecurity professionals say their organizations are governing the use of AI internally, expanding their management of AI, or planning to formally manage AI use within the next 12 months. This is compared with 45% of respondents who admit that they need to learn more before diving in (see figure 57).

FIGURE 56

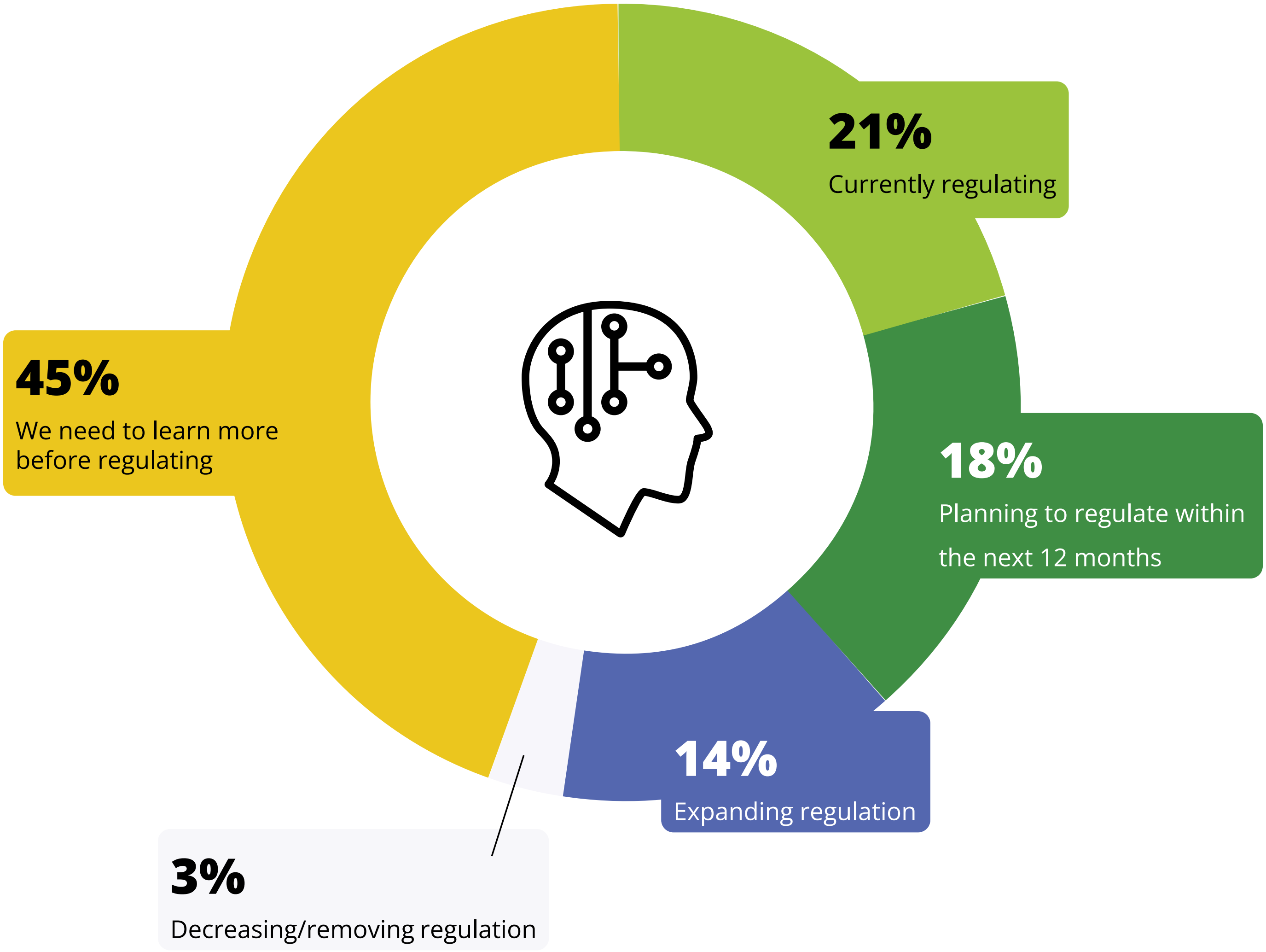
Which of the following emerging cybersecurity technologies/architectures do you believe will have the greatest positive impact on your ability to secure your organization?



Base: 14,865 global cybersecurity professionals
Note: Showing top three ranked

FIGURE 57

How has the increasing use and popularity of modern AI applications (e.g., ChatGPT) impacted your cybersecurity program from a regulatory standpoint?



Base: 11,735 global cybersecurity professionals
Note: "Don't know/does not apply" responses were removed from the sample base; Total percentages may not equal separate values due to rounding.

What It Means for Organizations

Preparing for the Future of Work

Cybersecurity professionals are weighing the potential opportunities and threats of tomorrow's technology — most notably, the impact of AI. As individuals and organizations alike approach AI with cautious optimism, one thing becomes increasingly clear — whether you are investing, regulating or avoiding AI completely, learning more about it is critical.

Here is our takeaway after speaking with cybersecurity professionals about AI:

- **AI education is critical before adoption.** 45% of cybersecurity professionals surveyed believe that within two years, AI will overtake worker/skill shortages as their top challenge. While we still don't know the full breadth of AI's potential impact on cybersecurity, we do know how little we know about it. 84% of respondents say that they have no/minimal knowledge or only some/moderate knowledge of AI/ML, and the gap in AI/ML skills is second only to the gap in cloud computing security. If the demand for this skill continues to increase, organizations will be left with no one skilled enough to manage or regulate it. Companies need to begin offering enterprise-wide AI training programs to nurture expertise on this emerging technology from within.

Conclusion

Cybersecurity professionals remain steadfastly focused on defending their organizations. However, our findings reveal increasingly stressed cybersecurity teams. Workforce gaps and skills deficits have made their jobs more challenging than ever. It is time for leaders in the public and private sectors to recognize that the cybersecurity workforce needs help. It is time to act.

The good news? Our study reveals that proactive organizations and leadership can make a powerful difference for their cybersecurity teams right now. Organizations that invest in their teams benefit from more engaged and satisfied workers dedicated to their mission despite mounting economic pressure, a heightened threat landscape and the uncertain, looming impact of emerging technologies such as AI.

Forward-thinking organizations are already shaping the future of cybersecurity by embracing new pathways into the field, blazing trails for the generations of cybersecurity professionals who follow. Data shows the powerful impact of more open-minded hiring practices, DEI initiatives and professional development reimbursements, as well as the negative impacts of layoffs on morale and security — but organizations can find a blueprint for success if they act on these findings. While times of economic uncertainty may result in organization-wide cutbacks, staffing reductions in cybersecurity contain significant risk. Any short-term financial gain will likely be quickly negated by financial and reputational loss from increased cyber risk or long-term vulnerability.

The private sector can’t do it alone. It is also time for lawmakers, policymakers and regulators around the world to listen to the cybersecurity workforce. Governments need to coordinate and harmonize efforts because cybersecurity is a global challenge. Cybersecurity professionals need supportive environments wherever they work, with sound policies that make sense and don’t add to the burden of already-understaffed teams. Policymakers are making tremendous progress in prioritizing cybersecurity, but equally important to the urgency needed to address these matters is to ensure these efforts become enablers for cybersecurity professionals and not obstacles. Governments and regulators must focus on encouraging a skilled workforce, providing the right tools and resources and most importantly, listening to and heeding professionals’ advice. Doing so is vital to successfully defending our critical assets around the world.

The 2023 ISC2 Cybersecurity Workforce Study saw our largest participation yet. Its insights create the foundation for smarter decisions and policies that will make meaningful and lasting contributions to a safe and secure cyber world.

Appendix A: Methodology

This year, our method compiles a variety of secondary data sources in combination with proprietary survey data to create a single, holistic estimate. This tactic of combining multiple different methodological approaches keeps any single number from disproportionately influencing the final estimate.

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 estimates of 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.

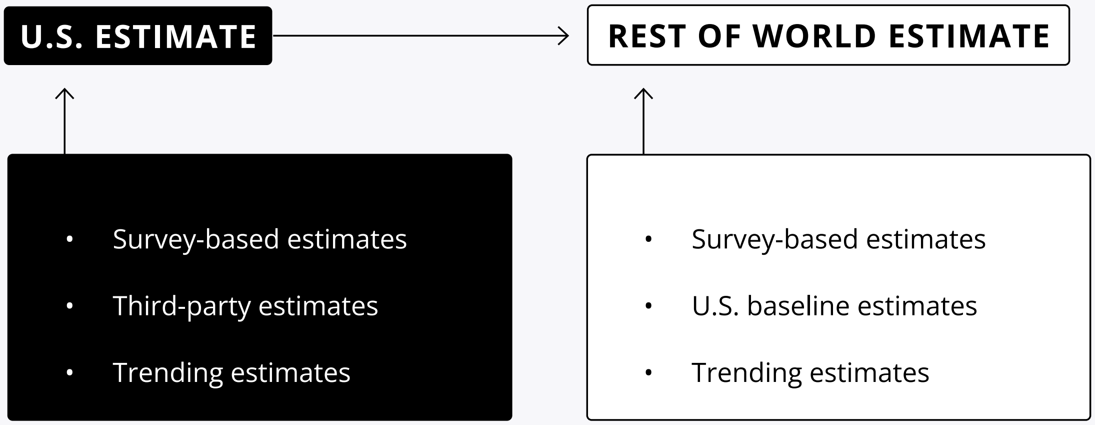
2. **Third-party estimates.** Various estimates of related populations were modified based on survey findings to match our estimation criteria. This includes the US Bureau of Labor Statistics' estimate of cybersecurity analysts.

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 except replacing third-party estimates for 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.

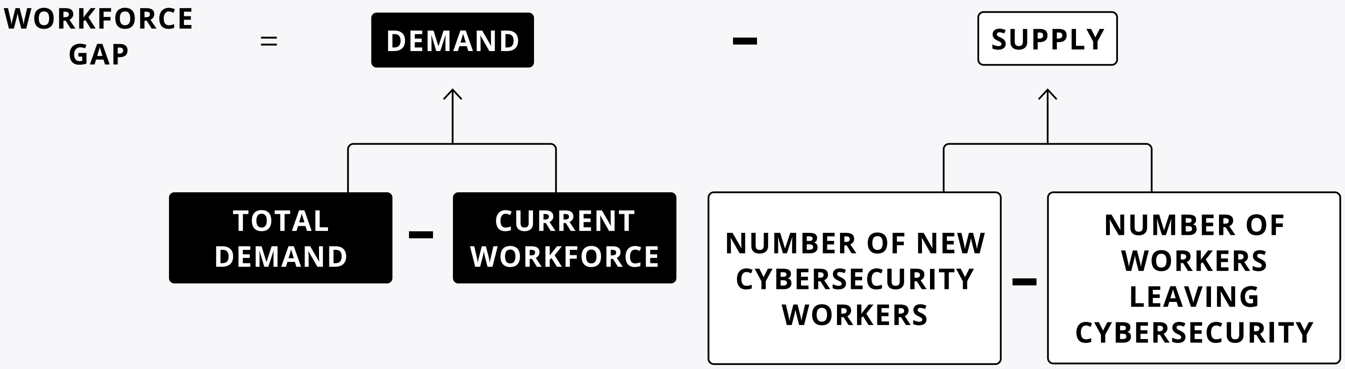
GAP ESTIMATE METHODOLOGY

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 equals demand minus 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 equals (total demand over the next 12 months minus the current workforce) minus (number of workers entering the field minus number of workers leaving the field).


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

Appendix B: Study Participant Demographics

COMPANY SIZE	
20,000 or more	**24%**
10,000-19,999	**8%**
5,000-9,999	**9%**
2,500-4,999	**9%**
1,000-2,499	**11%**
500-999	**10%**
250-499	**7%**
100-249	**7%**
50-99	**5%**
20-49	**3%**
10-19	**2%**
5-9	**1%**
2-4	**1%**
1 (independent contractor or self-employed)	**2%**

RESPONDENT LEVEL	
C-level executive	**5%**
Executive management	**6%**
Director/middle manager	**19%**
Manager	**22%**
Non-managerial mid- or advanced-level staff	**39%**
Entry/junior-level staff	**4%**
Independent contractor/ consultant	**4%**

INDUSTRY (TOP 10 SHOWN)	
IT services	**23%**
Financial services	**11%**
Government	**10%**
Consulting	**7%**
Military/military contractor	**7%**
Healthcare	**4%**
Telecommunications	**4%**
Manufacturing	**4%**
Security software/hardware development	**4%**
Education	**3%**

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

DEPARTMENT	
IT	**44%**
Security/privacy	**56%**

INTERNAL/EXTERNAL	
Internal security staff for my organization	**61%**
Security consultant or consultancy	**22%**
External security service provider (e.g., MSSP, external SOC, independent contractor etc.)	**12%**
Other	**6%**

HIRING AUTHORITY	
I make final decisions about hiring	**25%**
I am part of a team that makes hiring decisions	**25%**
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	**24%**

FULL TIME/PART TIME	
Employed/self-employed full-time	**93%**
Employed/self-employed part-time	**3%**
Retired	**1%**
Not currently working/ unemployed	**1%**
Prefer not to answer	**1%**

TIME SPENT ON SECURITY	
100% of a typical week	**18%**
75%-99%	**22%**
50%-74%	**25%**
25%-49%	**21%**
1%-24%	**13%**

AGE	
74 or older	**0.2%**
65-73	**2.0%**
60-64	**4.4%**
55-59	**8.5%**
50-54	**12.2%**
45-49	**15.5%**
39-44	**20.7%**
35-38	**13.0%**
30-34	**11.9%**
23-29	**6.7%**
Under 23	**0.3%**

COUNTRY	
United States (US)	40%
United Kingdom (UK)	7%
Japan	6%
Canada	5%
China	4%
Singapore	3%
Germany	3%
India	3%
Australia	3%
Netherlands	3%
South Korea	2%
France	2%
Spain	2%
Brazil	2%
South Africa	1%
Republic of Ireland	1%
United Arab Emirates	1%
Mexico	1%
Saudi Arabia	1%
Nigeria	1%
Hong Kong	1%
Switzerland	1%
Taiwan	1%
Other	3%

STATE (TOP 20 SHOWN)	
Virginia	9%
Texas	9%
California	8%
Maryland	6%
Florida	6%
Colorado	4%
New York	4%
Georgia	4%
Washington	3%
Illinois	3%
Pennsylvania	3%
Ohio	3%
North Carolina	3%
Massachusetts	2%
Arizona	2%
New Jersey	2%
Minnesota	2%
Washington, DC	2%
Michigan	2%
Alabama	2%

GENDER OF RESPONDENTS	
Female	16%
Male	77%
Intersex	0.2%
Transgender	0.3%
Nonbinary	0.3%
Prefer to self-describe	0.2%
Prefer not to say	6%

Note: Percentages may not total 100 due to rounding.

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 more than 500,000 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, to better understand the barriers facing the cybersecurity profession and to uncover solutions that enable individuals to excel in their profession, achieve their career goals and better secure their organizations' critical assets.

The 2023 ISC2 Cybersecurity Workforce Study is based on online survey data collected in collaboration with Forrester Research, Inc. in April and May 2023 from 14,865 individuals responsible for cybersecurity at workplaces throughout North America, Latin America (LATAM), the Asia-Pacific region (APAC) and Europe, Africa and the Middle East (EMEA). Respondents in non-English-speaking countries completed a locally translated version of the survey.

Learn more at www.isc2.org/research.