(ISC)^2 CYBERSECURITY WORKFORCE STUDY

A critical need for cybersecurity professionals persists amidst a year of cultural and workplace evolution

2022

Table of Contents

Executive Summary

2022 is a highly formative year for the cybersecurity profession. Shaped and defined by geo-political and macroeconomic turbulence, the obstacles of the modern cybersecurity landscape have galvanized passion and persistence within its workforce - which continues to change and evolve with the world around it. The global cybersecurity workforce is growing, but so is the gap in professionals needed to carry out its critical mission.

We estimate the size of the global cybersecurity workforce at 4.7 million people – the highest we've ever recorded. According to our research, however, the cybersecurity field is still critically in need of more professionals. To adequately protect cross-industrial enterprises from increasingly complex modern threats, organizations are trying to fill the **worldwide gap of 3.4 million cybersecurity workers**. To fully contextualize the state of cybersecurity in 2022, we'll analyze the field through multiple lenses.

At an enterprise level, the executive spotlight is pointed directly at cybersecurity teams, who are expected to adapt and protect their own organizations from mounting risks while complying with emerging technology and regulatory requirements. Employees are adapting their working style and routines to meet these modern challenges, but they themselves are also evolving from cultural, emotional, and educational perspectives, and these differences paint a nuanced picture of the values and motivations that drive their careers.

As individuals, cybersecurity professionals are passionate about what they do, and their organizations need to recognize this and bolster them with the tools they need to succeed and continue charting a path forward for the entire profession. It is clear in our study that corporate culture can be very impactful on an employee's experience and happiness on the job, which in turn affects the efficacy of their work.

The future of cybersecurity is defined by professionals evolving and persisting through the volatility of today's threat landscape. Traditional habits are being broken and diverse perspectives are entering the field, as the next generation uses new pathways to jump-start their careers.

In this report, the fifth annual (ISC)^2 Cybersecurity Workforce Study, we surveyed **11,779 international practitioners and decision-makers** to gain their unique perspectives and experiences about working in the modern cybersecurity profession. This report highlights hiring and recruiting trends, corporate culture and job satisfaction, career pathways, certifications, professional development, how the workforce is adapting to current events and what the future of cybersecurity work looks like.

Cybersecurity Workforce Gap & Estimate

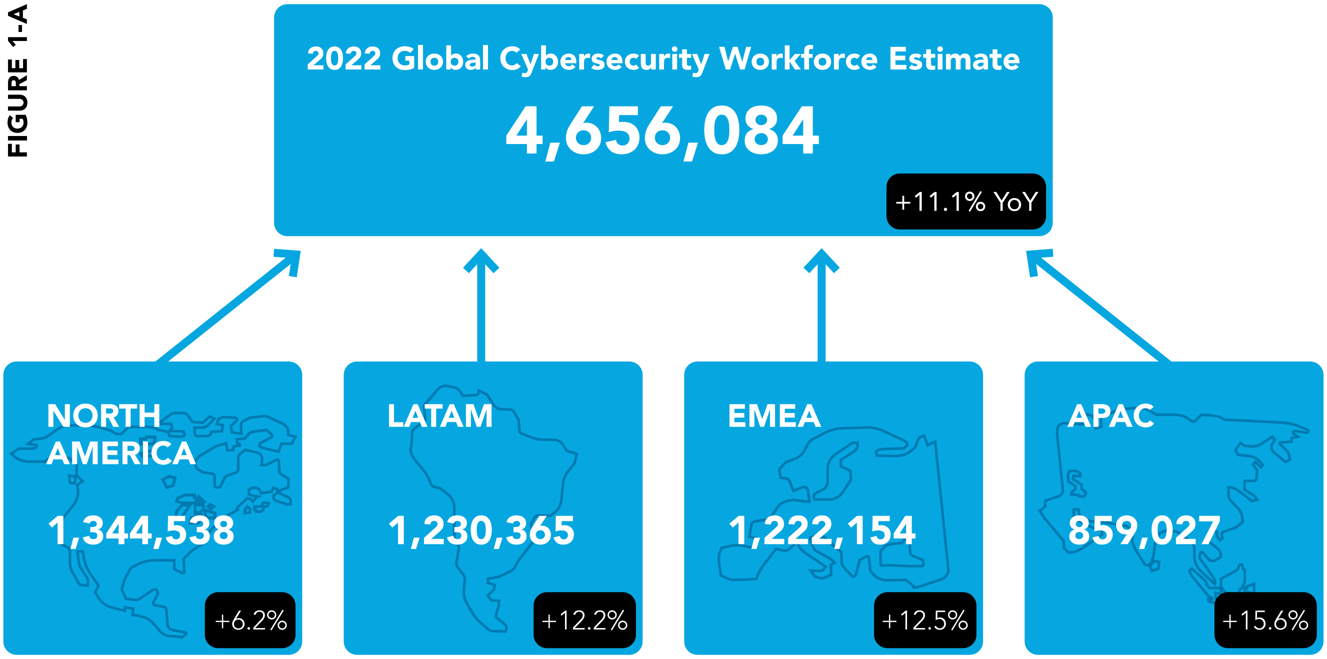
Before we can analyze the nuances and trends fueling change within the modern cybersecurity profession, it is paramount for us to understand the holistic nature of the field itself – how it is growing and scaling to meet the needs of organizations worldwide. **Calculating a global workforce estimate and gap are crucial to framing the remainder of this report.**

To understand the scope of cybersecurity professionals worldwide, (ISC)^2 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).

(ISC)^2 estimates the global cybersecurity workforce in 2022 at 4.7 million, an 11.1% increase over last year, representing 464,000 more jobs. We saw gains across all regions, with Asia-Pacific (APAC) registering the greatest growth (15.6%) and North America the least (6.2%) (see figures 1-A and 1-B).

Our study estimates the cybersecurity workforce of 14 countries in 4 regions (see Appendix A for more details).

FIGURE 1-A



2022 Global Cybersecurity Workforce Estimate

4,656,084

+11.1% YoY

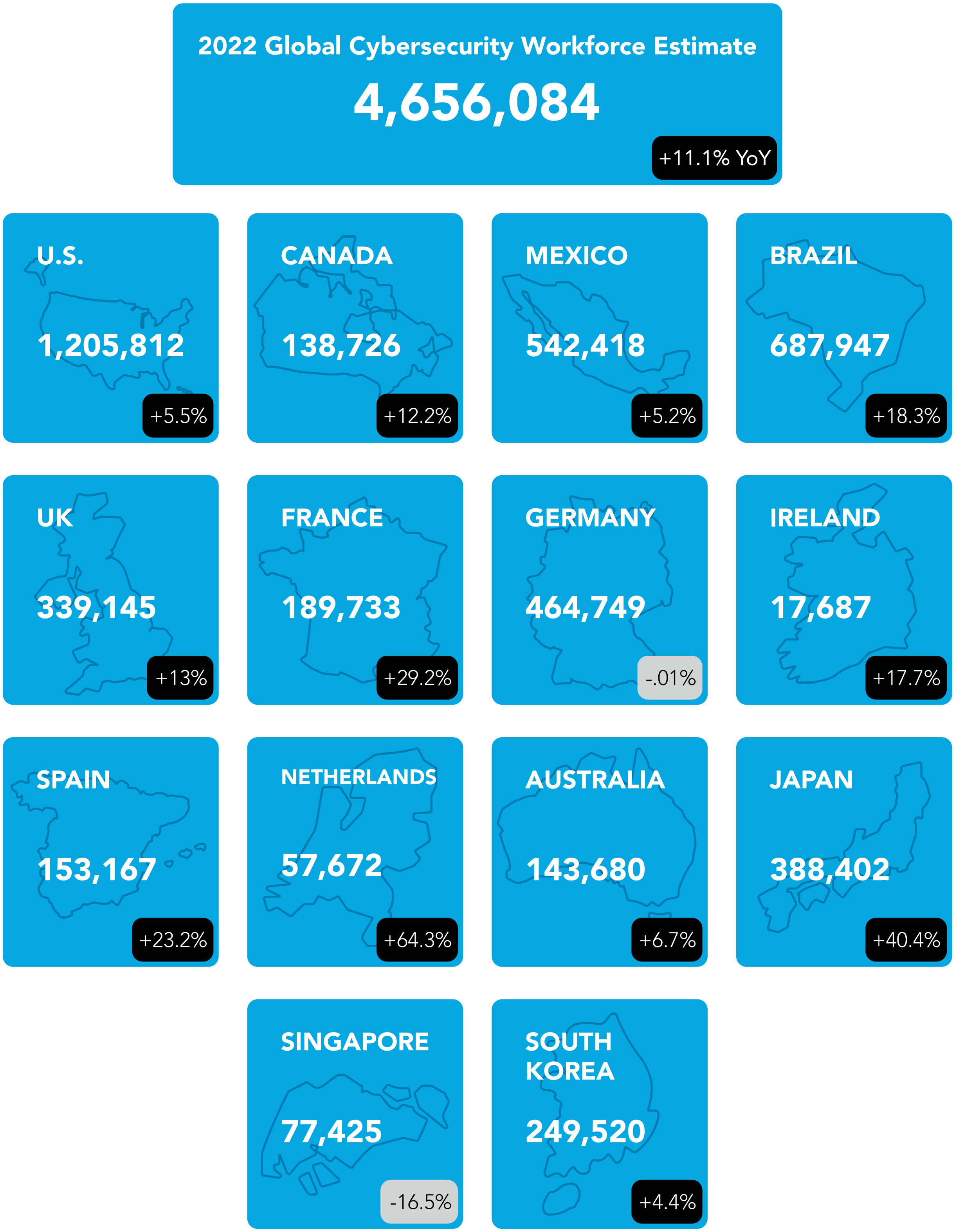
NORTH AMERICA 1,344,538 +6.2%

LATAM 1,230,365 +12.2%

EMEA 1,222,154 +12.5%

APAC 859,027 +15.6%

FIGURE 1-B



2022 Global Cybersecurity Workforce Estimate

4,656,084

+11.1% YoY

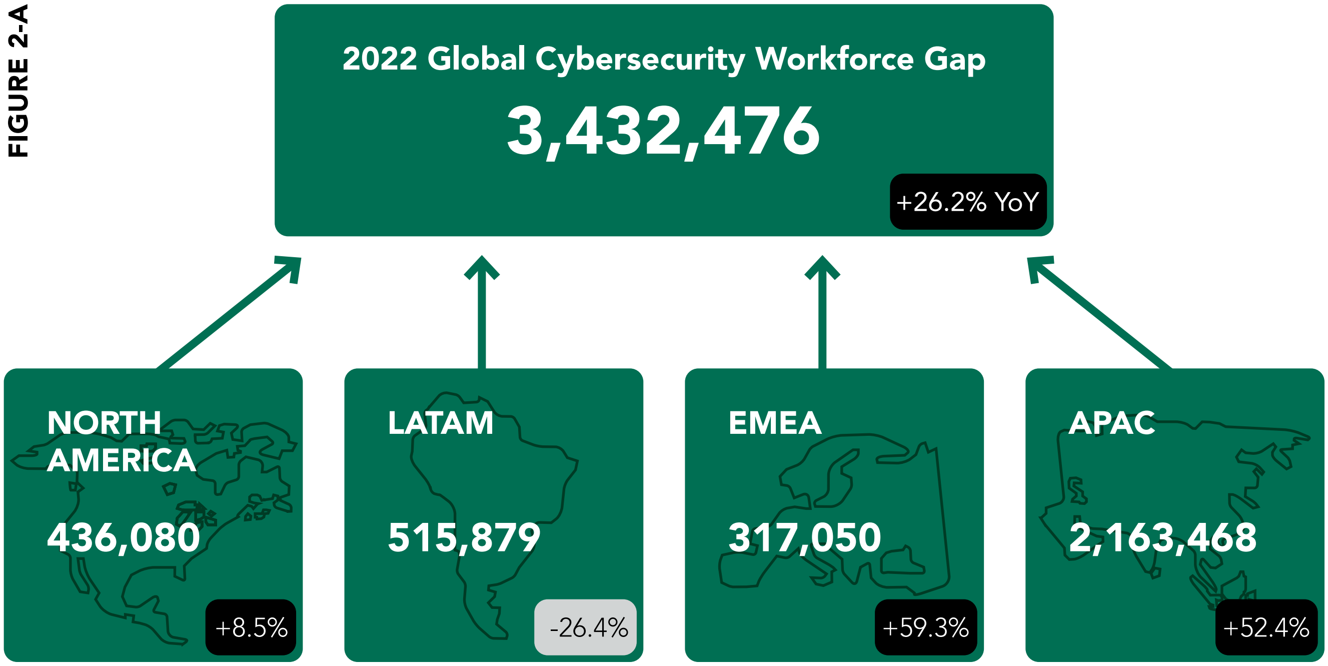
U.S.	1,205,812	+5.5%
CANADA	138,726	+12.2%
MEXICO	542,418	+5.2%
BRAZIL	687,947	+18.3%
UK	339,145	+13%
FRANCE	189,733	+29.2%
GERMANY	464,749	-.01%
IRELAND	17,687	+17.7%
SPAIN	153,167	+23.2%
NETHERLANDS	57,672	+64.3%
AUSTRALIA	143,680	+6.7%
JAPAN	388,402	+40.4%
SINGAPORE	77,425	-16.5%
SOUTH KOREA	249,520	+4.4%

While the cybersecurity workforce is growing rapidly, demand is growing even faster. (ISC)²'s cybersecurity workforce gap analysis revealed that despite adding more than 464,000 workers in the past year, the cybersecurity workforce gap has grown more than twice as much as the workforce with a 26.2% year-over-year increase, making it a profession in dire need of more people (see figures 2-A and 2-B).

> Despite adding more than 464,000 workers in the past year, the cybersecurity workforce gap has grown more than twice as much as the workforce.

Our study estimates the cybersecurity workforce gap for 16 countries in 4 regions (see Appendix A for more details).

FIGURE 2-A



2022 Global Cybersecurity Workforce Gap
3,432,476
+26.2% YoY

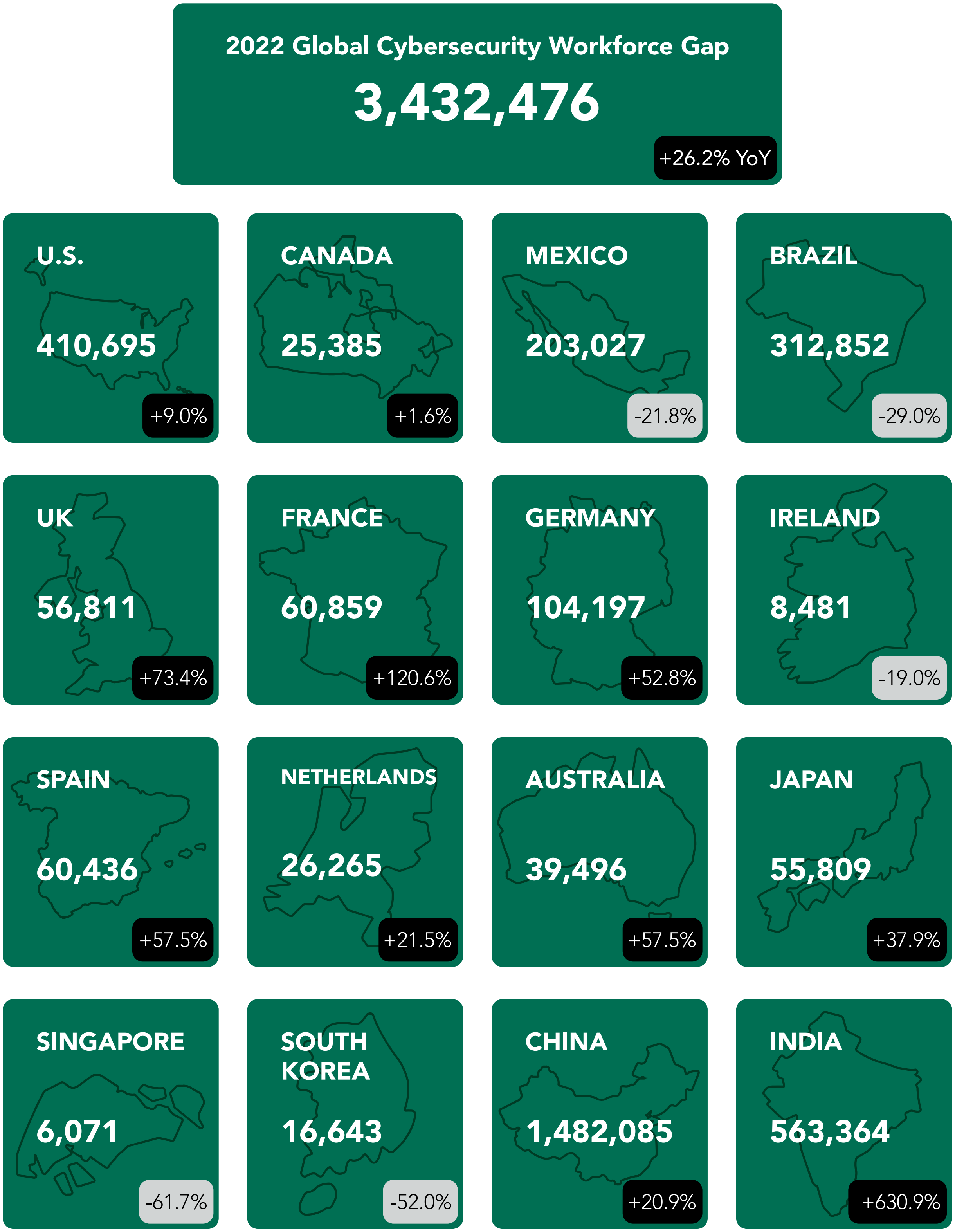
NORTH AMERICA
436,080
+8.5%

LATAM
515,879
-26.4%

EMEA
317,050
+59.3%

APAC
2,163,468
+52.4%

FIGURE 2-B



2022 Global Cybersecurity Workforce Gap

3,432,476

+26.2% YoY

U.S.
410,695
+9.0%

CANADA
25,385
+1.6%

MEXICO
203,027
-21.8%

BRAZIL
312,852
-29.0%

UK
56,811
+73.4%

FRANCE
60,859
+120.6%

GERMANY
104,197
+52.8%

IRELAND
8,481
-19.0%

SPAIN
60,436
+57.5%

NETHERLANDS
26,265
+21.5%

AUSTRALIA
39,496
+57.5%

JAPAN
55,809
+37.9%

SINGAPORE
6,071
-61.7%

SOUTH KOREA
16,643
-52.0%

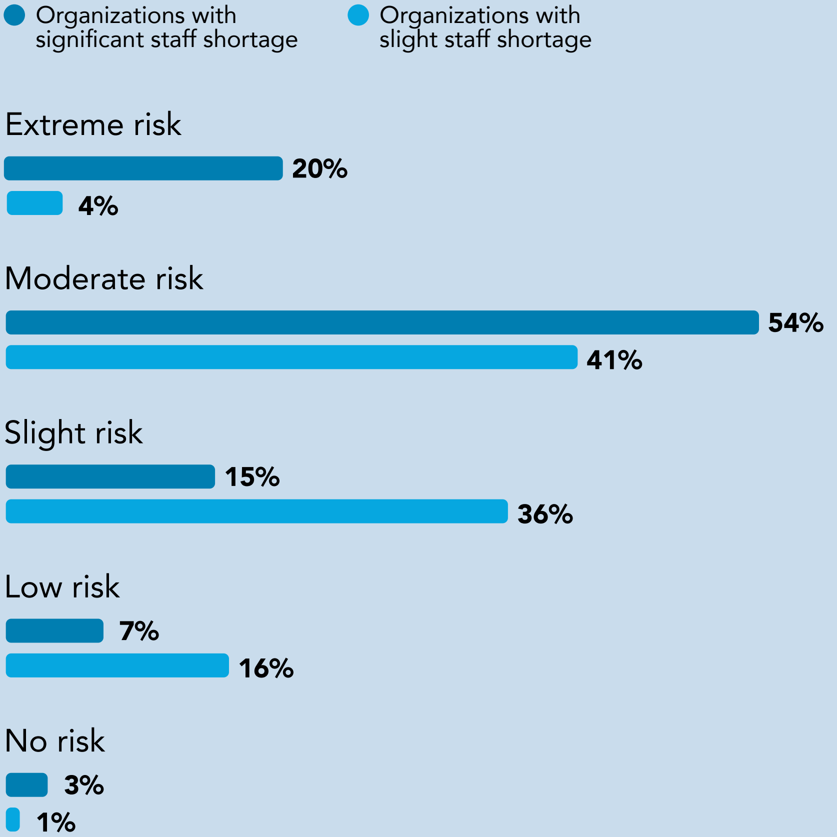
CHINA
1,482,085
+20.9%

INDIA
563,364
+630.9%

The workforce gap is not going unnoticed by cybersecurity workers – nearly 70% feel their organization does not have enough cybersecurity staff to be effective. The shortage is particularly severe in aerospace, government, education, insurance and transportation. A cybersecurity workforce gap jeopardizes the most foundational functions of the profession like risk assessment, oversight and critical systems patching. More than half of employees at organizations with workforce shortages feel that staff deficits put their organization at a "moderate" or "extreme" risk of cyberattack. And that risk increases substantially when organizations have a significant staffing shortage (see figure 3).

FIGURE 3

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

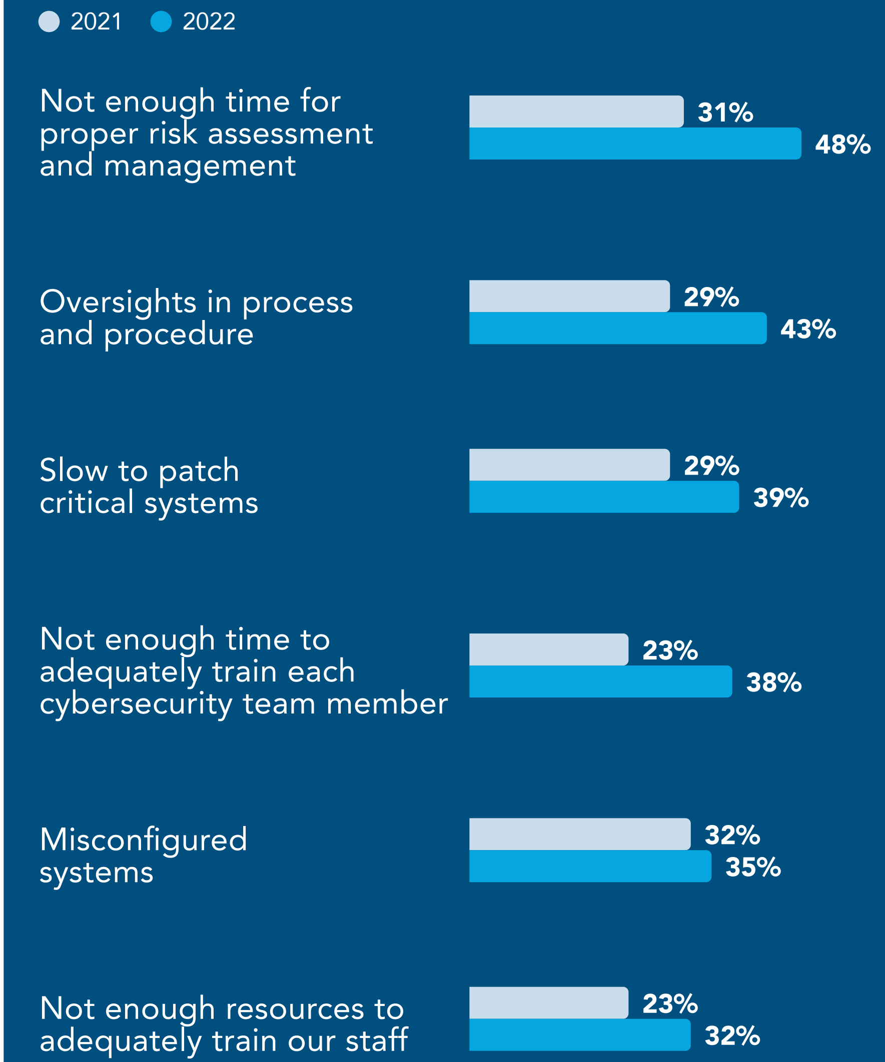


Base: 4,967 global cybersecurity professionals whose teams have staff shortages

In many areas, our study found that the workforce gap is being felt by employees more than ever. Compared with last year, far more cybersecurity professionals indicated that their organization had experienced issues like lacking proper time for assessment and oversight of processes, slow patching of critical systems and inadequate time and resources for training as a consequence of staffing shortages (see figure 4).

FIGURE 4

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



Base: 4,967 global cybersecurity professionals whose teams have staff shortages

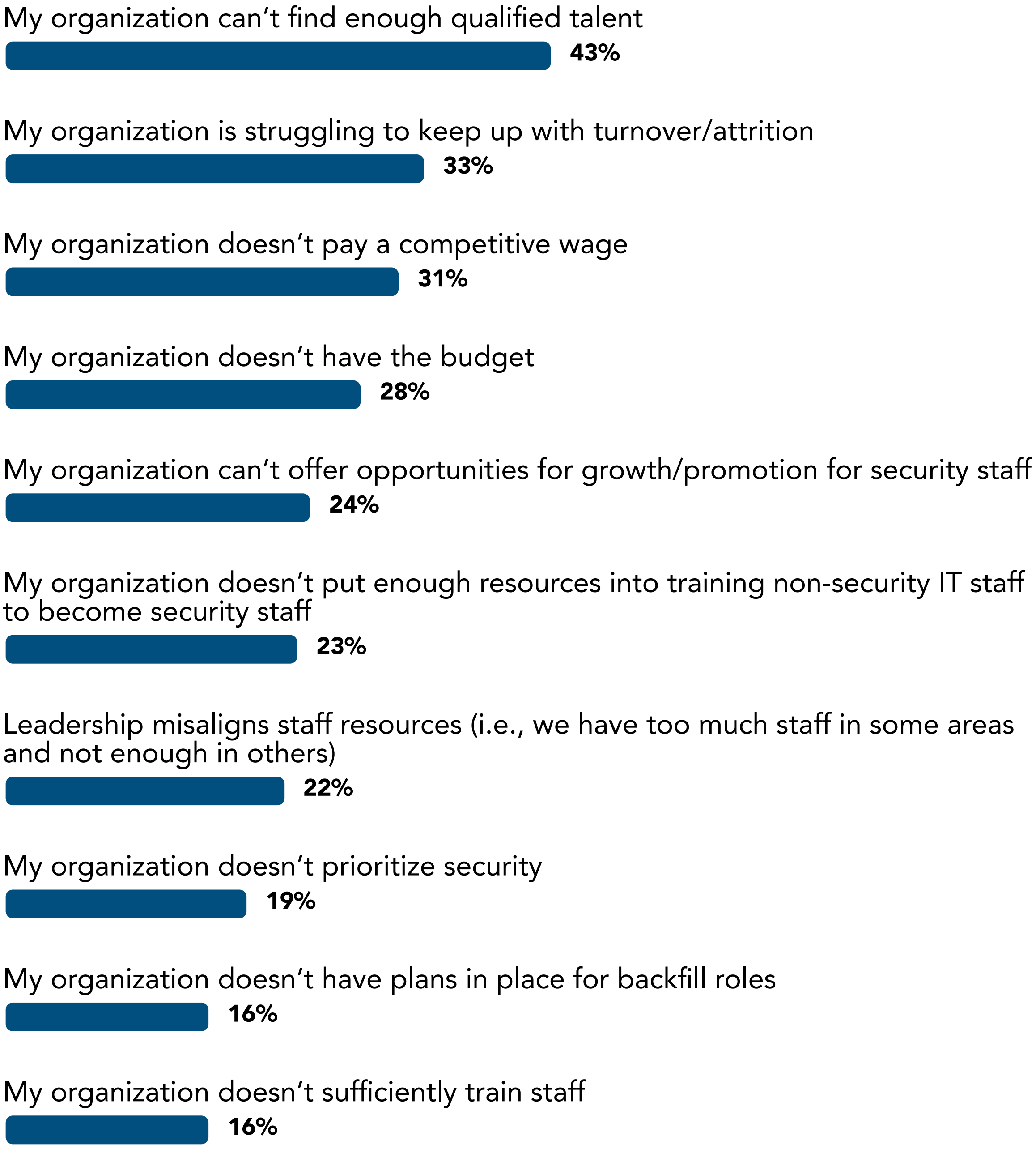
ADDRESSING THE WORKFORCE GAP

Why does this workforce gap exist? How can organizations best mitigate it? Some factors are certainly out of an organization's control – demand for cybersecurity employees is bound to increase as the threat landscape continues to grow in complexity and supply can't always keep up. Indeed, the inability to find qualified talent was cited most frequently as a challenge by organizations with cybersecurity staff shortages (see figure 5). Yet while this may be the most common challenge, it is not necessarily the most impactful.

To better understand what challenges are linked to the biggest staffing shortages, we examined what percentage of employees at organizations with those issues had significant staffing shortages. This analysis suggests that the most negatively impactful issues are ones that organizations can indeed control: not prioritizing cybersecurity, not sufficiently training staff, and not offering opportunities for growth or promotion. Being unable to find qualified talent was actually the least impactful problem based on this analysis.

FIGURE 5

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



Base: 4,967 global cybersecurity professionals whose teams have staff shortages

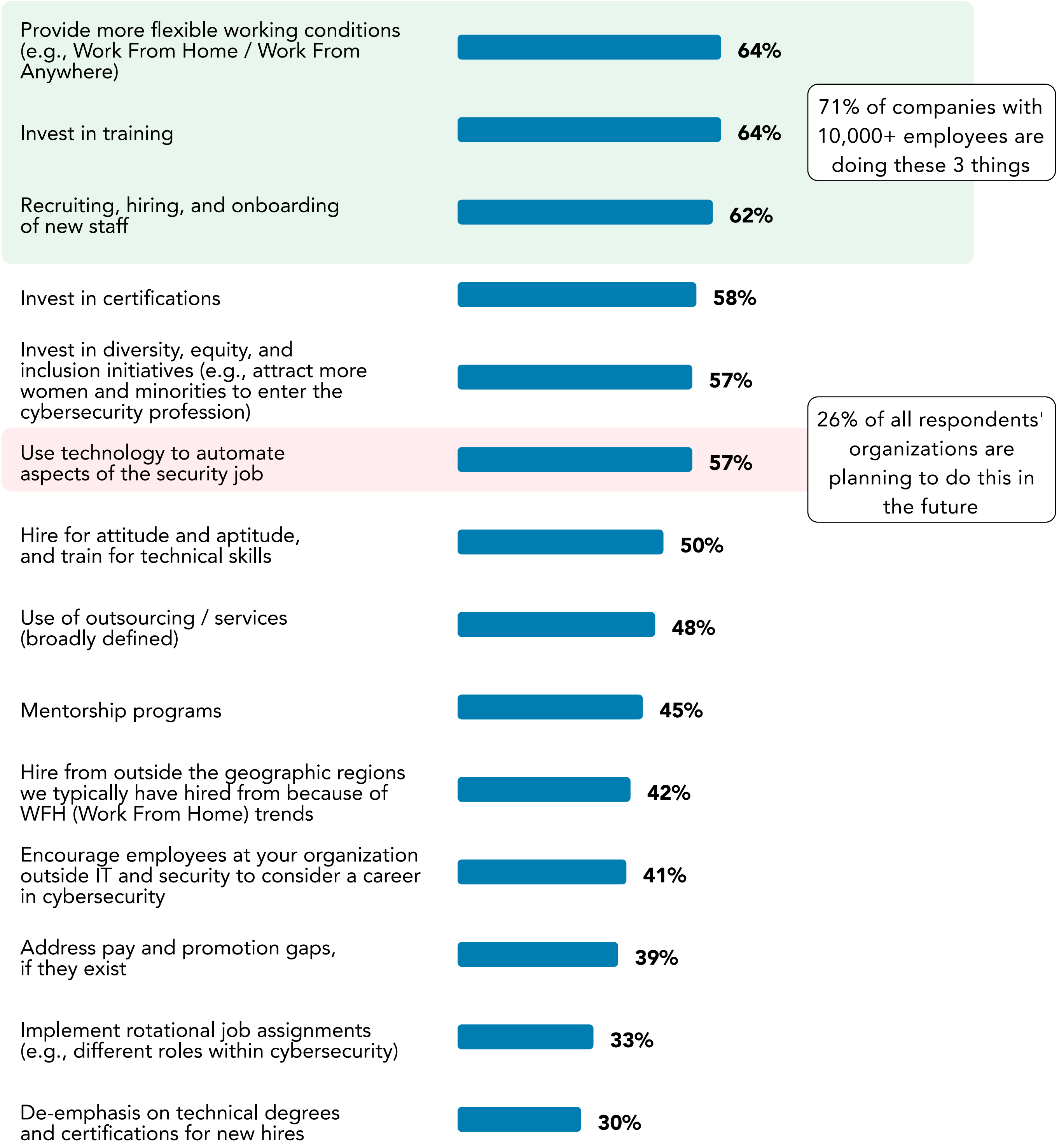
When we take a look at what is actually being done to address worker shortages, we can see that organizations are indeed putting in the effort to mitigate staff shortages (see figure 6). However, what they are doing is not always what is most effective. Although almost all initiatives had a positive impact on staffing, we found that organizations with initiatives to train internal talent – rotating job assignments, mentorship programs and encouraging employees outside of cybersecurity to join the field – were least likely to have shortages (see figure 7). These initiatives are particularly impactful for larger companies – only 49% of companies with 1,000 or more employees who had implemented all three of these internal training initiatives had staffing shortages compared with 77% of those who had implemented none.

These were not, however, the most commonly adopted initiatives. In fact, many of the most effective initiatives had the lowest implementation levels. The initiative with by far the lowest impact is outsourcing. Respondents at organizations who were outsourcing cybersecurity were actually slightly more likely to see a shortage in staff.

Automation is becoming more prevalent in cybersecurity as well – 57% have adopted it today and an additional 26% plan to adopt it in the future – and while it isn't likely to take the place of cybersecurity workers at any time in the foreseeable future, automating processes that are consistent and repeatable frees up workers to focus on higher-level tasks. This may reduce staffing shortage issues without requiring additional staff.

FIGURE 6

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



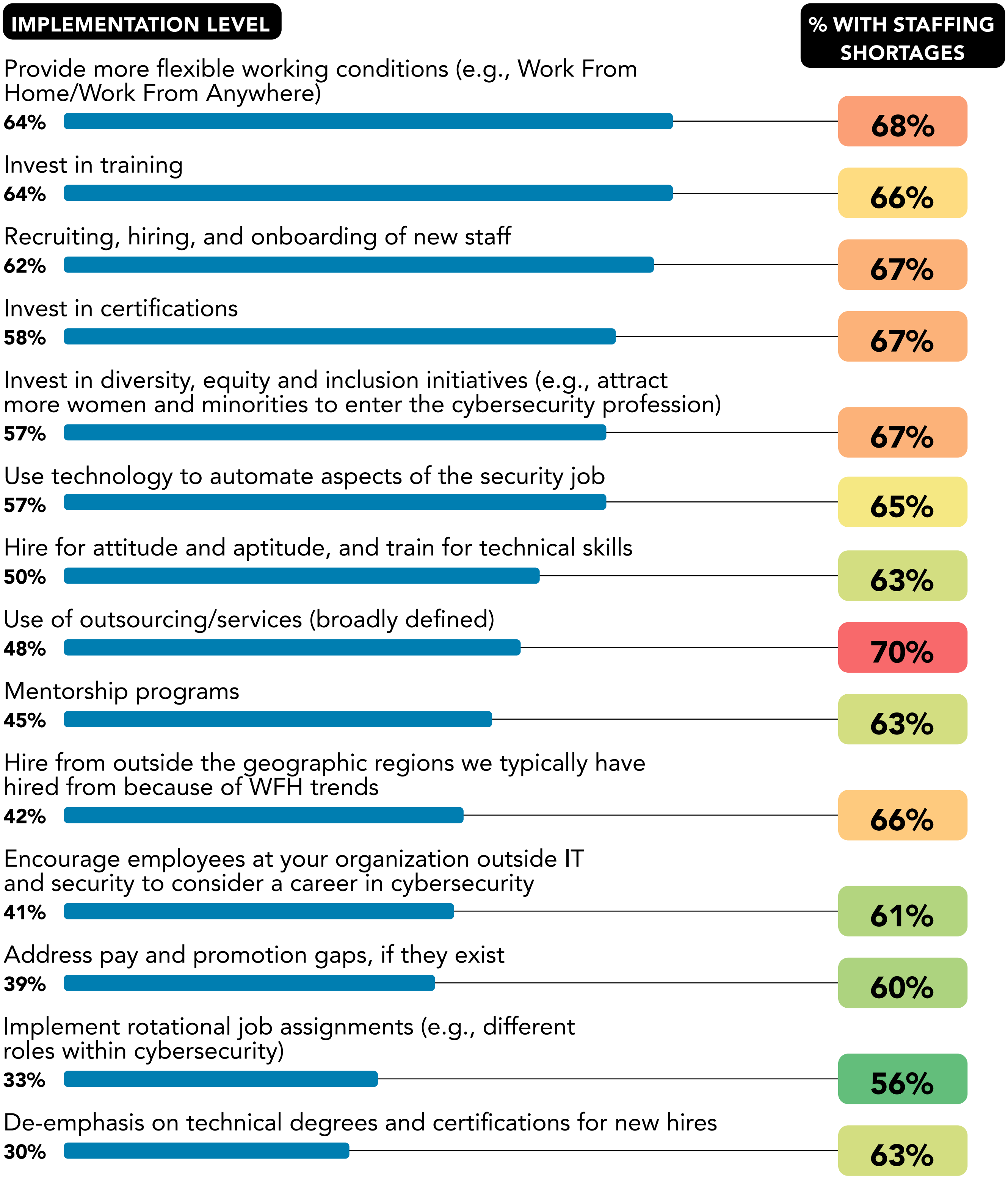
71% of companies with 10,000+ employees are doing these 3 things

26% of all respondents' organizations are planning to do this in the future

Base: 11,525 global cybersecurity professionals on cybersecurity teams

FIGURE 7

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



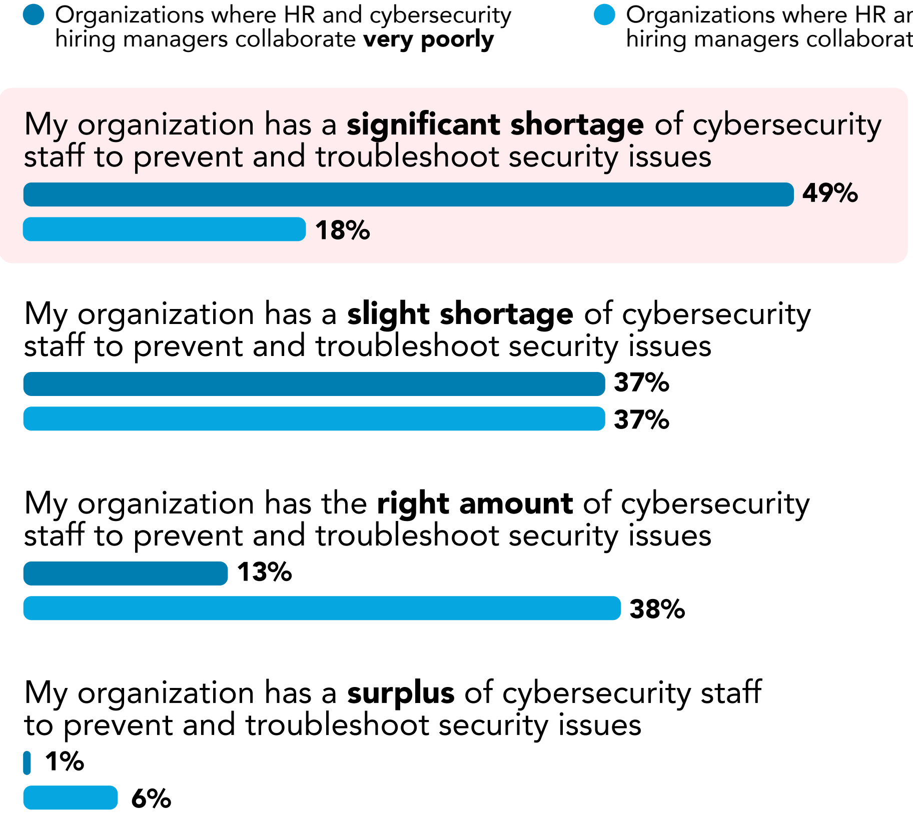
Base: 11,525 global cybersecurity professionals on cybersecurity teams

When it comes to hiring, cybersecurity managers can't work alone. The study finds that cybersecurity hiring managers who had a strong working relationship with their HR department were far less likely to have significant staffing shortages at their organizations (see figure 8). However, only 52% of respondents said that hiring managers have a strong working relationship with HR, and 40% of hiring managers said that the HR department at their organization does not add value to the recruiting process.

> Cybersecurity hiring managers who had a strong working relationship with their HR department were far less likely to have significant staffing shortages at their organizations.

FIGURE 8

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



Base: 7,529 global cybersecurity professionals on in-house cybersecurity teams

WHAT IT MEANS FOR ORGANIZATIONS

THE CYBERSECURITY WORKFORCE GAP

Cybersecurity workers are in greater demand than they've ever been before and supply can't keep up. The global workforce gap increased by over 25% this year and nearly 70% of organizations say they have a worker shortage. Combatting staffing shortages is no easy task but findings from our research yield some key places where organizations can focus:

- **Understand what your gap is.** Senior-level practitioners in our study were more likely than managers or executives to say their organization had a staffing shortage. This suggests that those making decisions may not always have a full appreciation of what front-line cybersecurity professionals are experiencing. Decision-makers should make sure they are actively listening to employees to understand if and where there are staffing shortages.

- **Emphasize internal training.** Our study found that the most impactful organizational initiatives in reducing worker shortages were those that took advantage of internal talent with programs like rotational job assignments, mentorship and encouraging non-IT employees at the organization to learn about cybersecurity. This was particularly true for larger organizations that may have more internal talent; it's just a matter of finding and honing it. The challenges that were most associated with high staffing shortages were a lack of emphasis organization-wide on cybersecurity, insufficient staff training and a lack of pathways for growth.

- **Work with HR, not against them when hiring for cybersecurity.** Hiring is a challenging process. While cybersecurity hiring managers likely know best what kinds of candidates to look for, HR managers are more likely to have the expertise on finding and attracting those candidates. Therefore, it's crucial for cybersecurity organizations to build effective working relationships with HR. Those who don't were more than 2.5x as likely to have significant staffing shortages compared with those who have built a strong relationship with HR.

Cybersecurity Team Culture

Company culture heavily defines employee experience. It shapes the social environment that employees operate in. It impacts how they communicate and collaborate with colleagues within their own team and across the organization. And it can influence how satisfied and supported they feel by their employer at large, ultimately influencing answers to the question of "should I stay, or should I go?"

Staff shortages are a common challenge in the post-pandemic cybersecurity environment. Many cybersecurity employees are being given increased flexibility and the freedom to choose where and how they work. People are seeking out work cultures that fit their lifestyles the best, and this has led to increased turnover. **21% of respondents from North America have switched organizations in the last 12 months; this is up from 13% in the previous year.**

For modern cybersecurity professionals, the definition of "corporate culture" is changing as pre-pandemic norms are being shattered and geographical lines are being blurred. In this critical area of our research, we analyzed employee experience within cybersecurity, and particularly how workplace trends and cultural nuances impact motivations, social values and employee satisfaction. Although overall satisfaction with cybersecurity work continues to be high, organizations may not be doing all they can to maximize employee experience. For example, cultural divides between junior and senior employees are widening, especially when it comes to the perceptions of diversity, equity and inclusion.

UNDERSTANDING CYBERSECURITY EMPLOYEE EXPERIENCE

Amidst a year of great change, we examined the cultural landscape of modern cybersecurity professionals and found:

FOR MANY, JOB SATISFACTION REMAINS HIGH.

Respondent satisfaction was lower, however, with their specific teams (68%), departments (62%), and overall organization (60%). Unhappiness tended to come from workplace culture and issues, rather than from cybersecurity work itself. Many who left their jobs over the past two years cited higher pay and more growth opportunities. But, concerningly, the next three reasons for leaving a job are all related to workplace conditions: negative culture, burnout and poor work/life balance (see figure 9). Overall, only 50% of those polled saw a high likelihood they would remain at their current organization for the next five years.

> Roughly 75% of those surveyed report being "somewhat satisfied" or "very satisfied" with their job and passionate about their work.

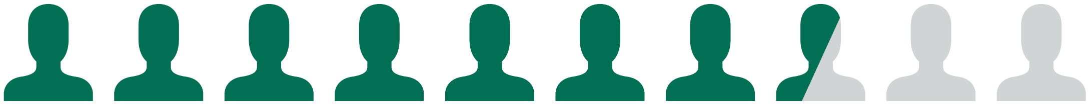
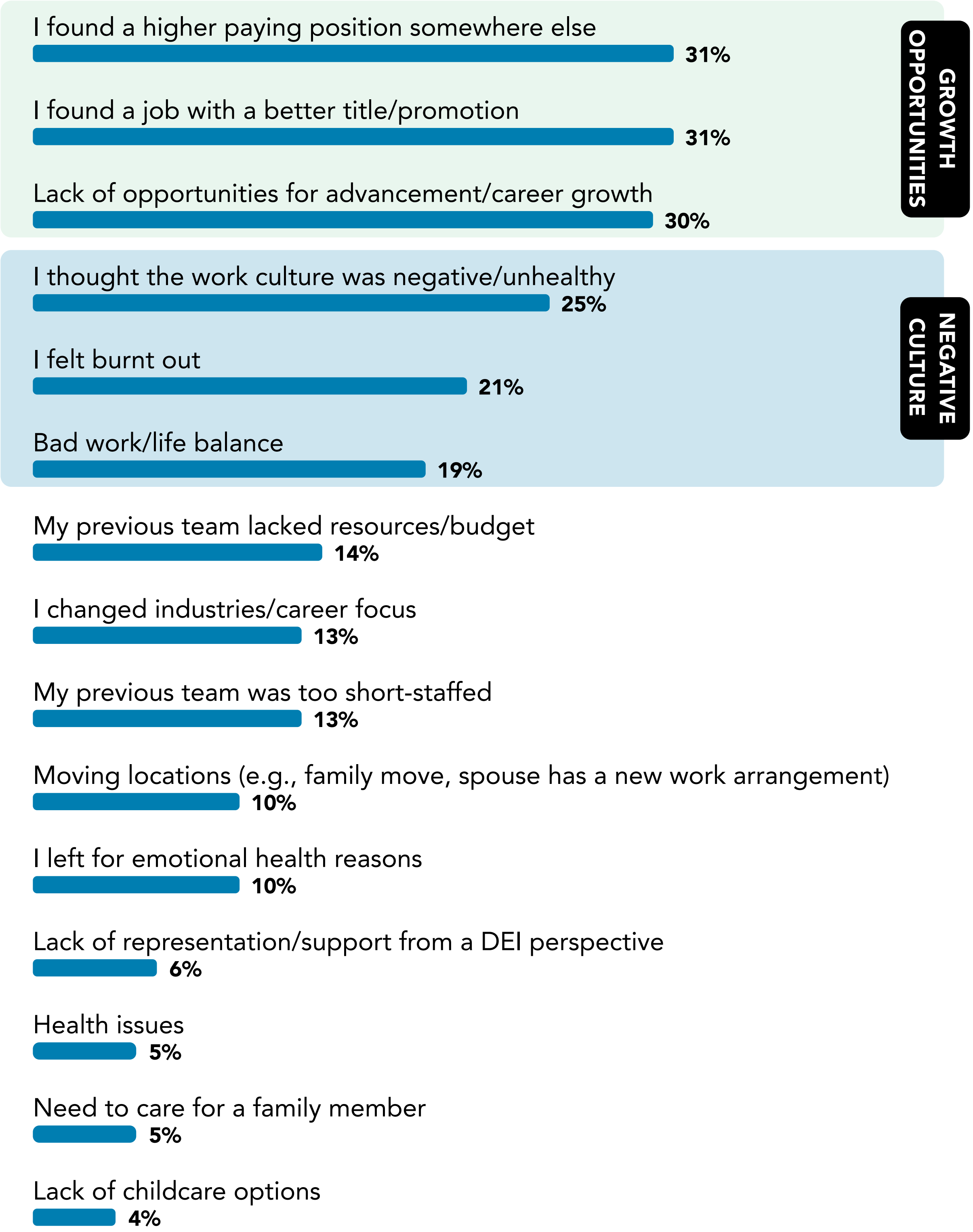


FIGURE 9

You indicated that you left a job within the past two years, what were the biggest reasons behind you making this move?



Base: 5,102 global cybersecurity professionals who have worked in their current role for 2 or fewer years

RATING EMPLOYEE EXPERIENCE

To better understand what affects the satisfaction and overall experience of cybersecurity workers, we developed a rating system that examines a variety of key factors, including engagement in work, feeling worn out at the job, sense of being fairly evaluated, and more. The Employee Experience (EX) rating system uses a scale from 100 (excellent) to 0 (terrible). For ease of evaluation, we grouped respondents into three categories based on their scores – “High EX,” “Medium EX” and “Low EX.” In this study, we will mainly evaluate the extremes, that is, high versus low. We’ll use the EX rating throughout this report to quantify results and provide a valuable data foundation for our recommendations.

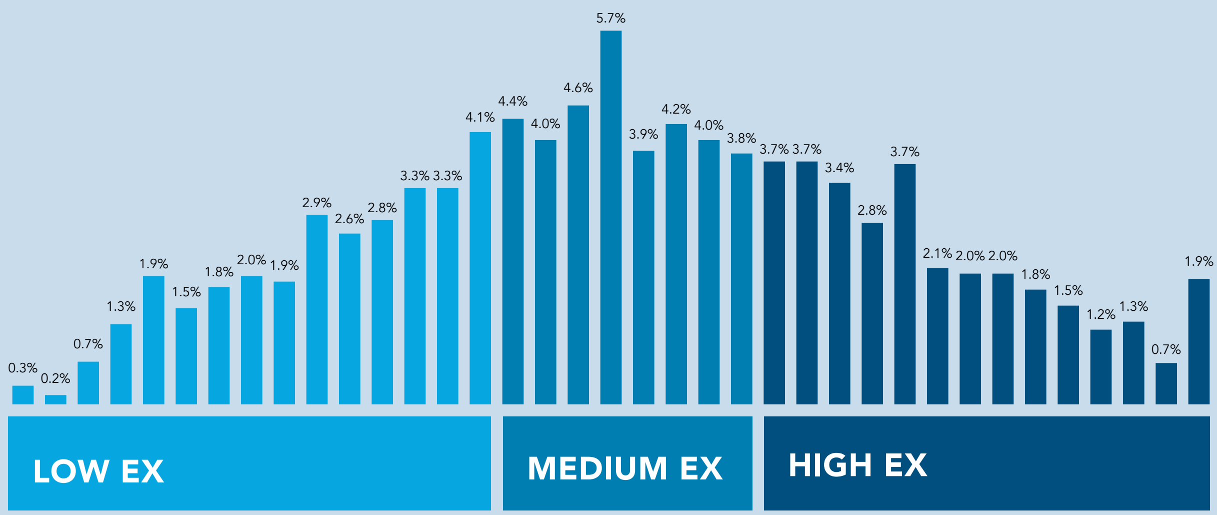
Employee Experience Rating

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

		SCORE	N
HIGH EX	Employees with high level of happiness at their work	**62 and above**	**3,822** (32.6%)
MEDIUM EX	Employees with a medium level of happiness at their work	**42 - 61**	**4,175** (35.6%)
LOW EX	Employees with a low level of happiness at their work	**41 and below**	**3,716** (31.7%)

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

Defining Employee Experience Rating



MOST RESPONDENTS LIKE CYBERSECURITY WORK, BUT UNHAPPINESS WITH ORGANIZATIONS FUELS STAFFING SHORTAGES

The analysis of responses on corporate culture, through the lens of EX ratings, provides evidence on what drives poor employee experience and satisfaction. We found:

- **Low scores were generally driven by organizational issues, not with the cybersecurity work itself.** High EX employees expressed greater passion for cybersecurity work, as compared to their Low EX colleagues. The differences between the groups became far greater when it came to satisfaction with their teams, organizations and departments (see figure 10). In fact, 60% of Low EX workers agreed that they like cybersecurity work but are not satisfied with their team/organization; this is compared with just 16% of their High EX counterparts (see figure 12).
- **Low EX is very harmful to organizations.** The data suggests that poor EX is a major contributor to staffing shortages. Compared to their higher-scoring peers, Low EX employees indicate they are far less motivated and productive at work and are much less likely to remain at their organizations for long (see figure 11).

FIGURE 10

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

(Percentage showing High/Very High responses)

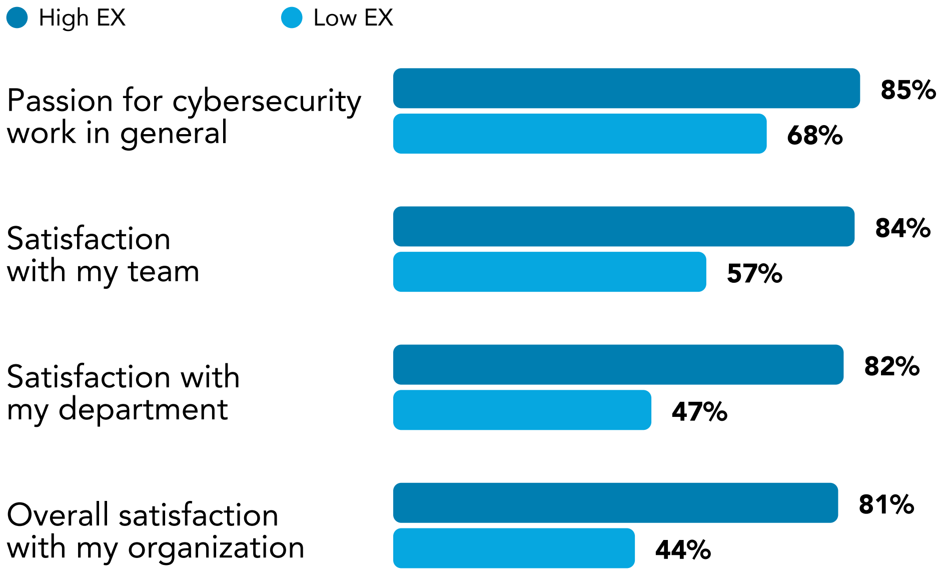
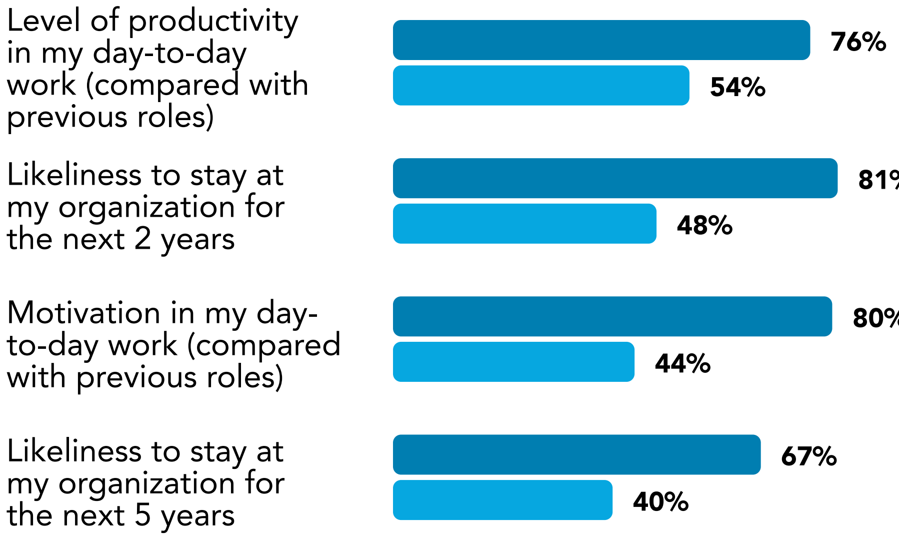


FIGURE 11



Base: 11,086-11,779 global cybersecurity professionals

TOP FACTORS INFLUENCING EMPLOYEE EXPERIENCE

Our survey results strongly suggest that EX and satisfaction are closely tied to organizational culture. But what are the most impactful factors driving both high and low scores? To identify and understand these, we first looked at the most common issues faced by respondents, as well as the initiatives their organizations have put in place to respond to these challenges. We then examined the average EX rating of respondents who selected each issue to see what resulted in the lowest and highest ratings. We found:

- **Not inviting and valuing worker input significantly contributes to poor EX.** Respondents were asked what issues negatively impacted their job satisfaction. The most common answer was having "too many emails/tasks." This is unsurprising, considering the prevalence of staffing shortages. However, employees being overworked, whether that's related to inadequate staffing or not, did not negatively affect EX scores nearly as much as a variety of cultural and organizational issues.

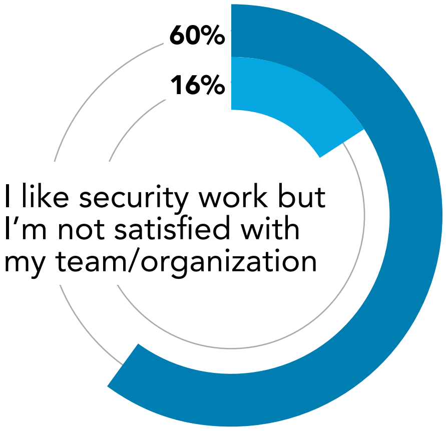
  The most significant factor of poor EX was the failure of organizations to listen to or value employee input (see figure 13). Cybersecurity professionals are passionate about their work, so while overwork is not a positive thing, it is not as negative as feeling like their expertise and knowledge are not being valued or asked for. The data shows that this impact is felt particularly with older workers who may feel like their experience has earned them the right to have a voice in the industry and their organization. When these employees are not listened to, they do not feel valued.

FIGURE 12

How much do you agree or disagree with the following statements about your security team's culture in general?

(Percentage showing Agree/Completely Agree responses)

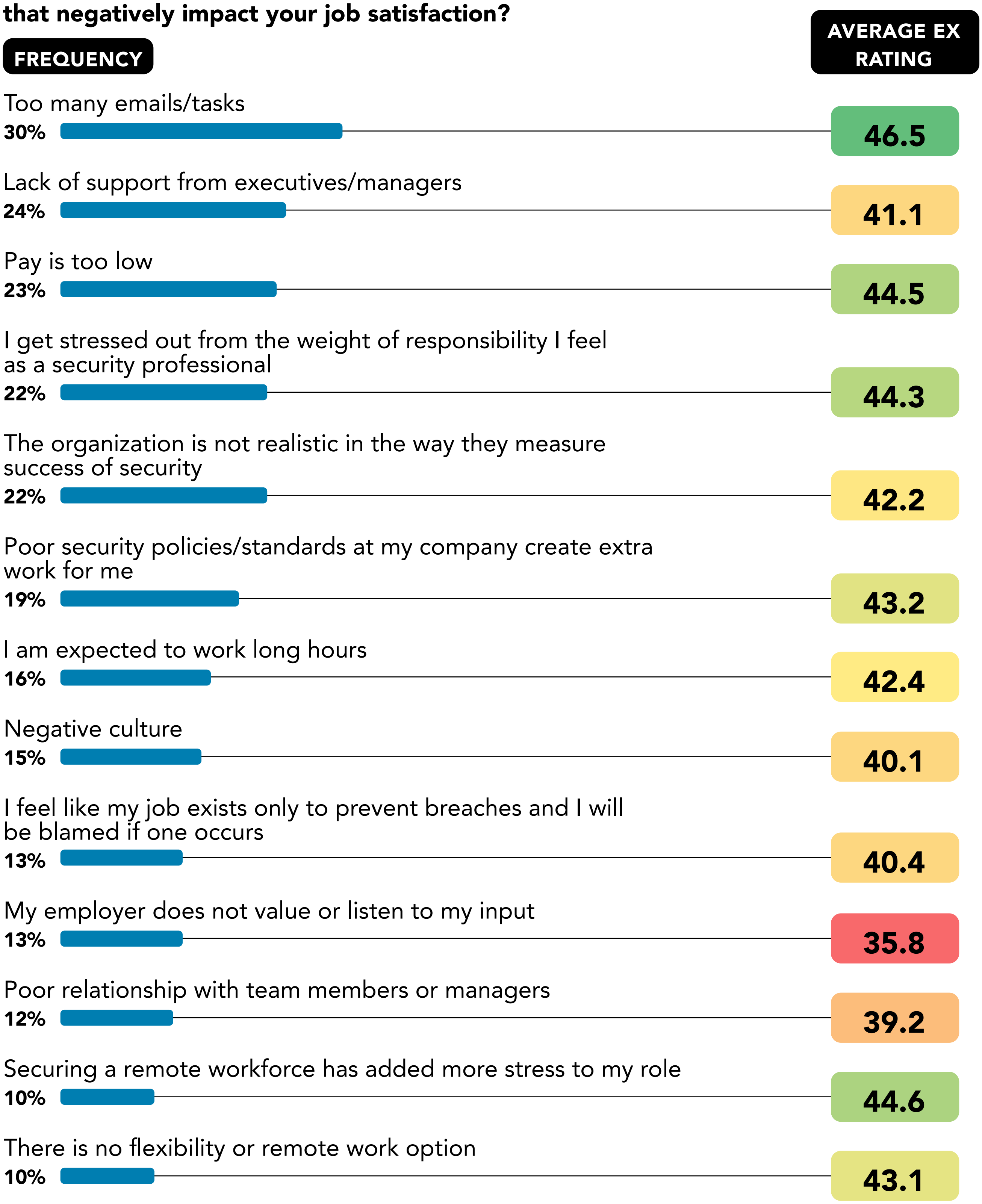
● High EX ● Low EX



Base: 11,525 global cybersecurity professionals on cybersecurity teams

FIGURE 13

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



Base: 11,525 global cybersecurity professionals on cybersecurity teams

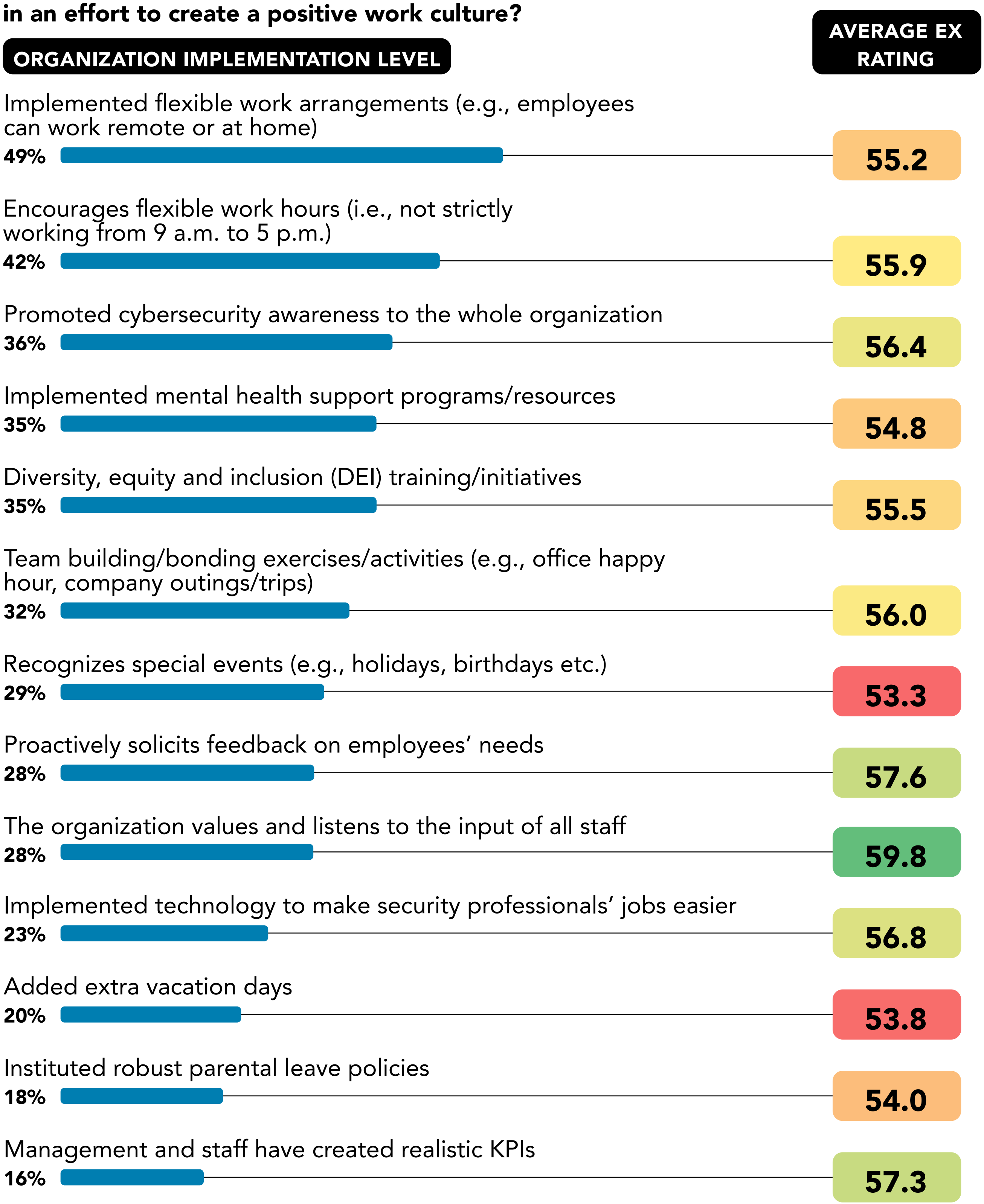
- **Organizations that make employees feel heard have happier personnel.** On the flip side, the most common initiatives that organizations have implemented to improve employee EX are centered around work flexibility, including remote work. However, such programs, while now considered essential accommodations by many workers, are not the most impactful. Instead, efforts to value the input of all employees produced the highest average EX rating (see figure 14). This is unfortunately not common, as only 28% report their organizations actively listen to and value the input of all staff.

  The next most beneficial initiative, proactively soliciting feedback on employees' needs, is similarly not widespread with only 35% reporting their organizations doing so.

  According to respondents, the addition of extra vacation days and recognizing birthdays and other special events were the least impactful initiatives. Additionally, the institution of robust parental leave policies was also near the bottom in terms of average EX, though it was far more impactful for cybersecurity workers in their 30s, especially women.

FIGURE 14

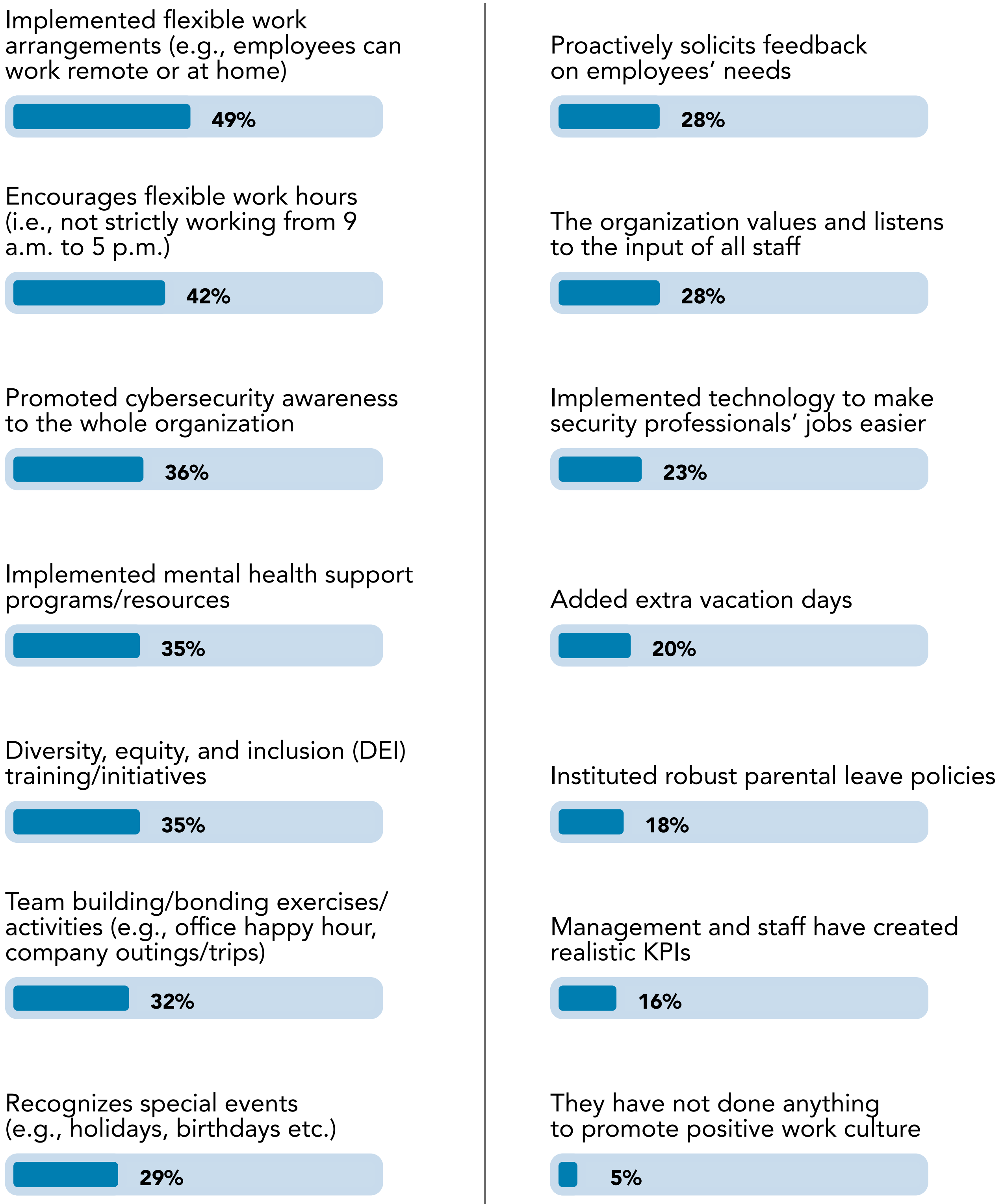
Which of the following has your organization done in an effort to create a positive work culture?



Base: 11,525 global cybersecurity professionals on cybersecurity teams

FIGURE 15

Which of the following has your organization done in an effort to create a positive work culture?



Base: 11,525 global cybersecurity professionals on cybersecurity teams

WILDLY POPULAR, REMOTE WORK DOUBLES TO 55% ADOPTION

As previously noted, the most common initiative organizations have implemented to create a positive work culture is changing where and when employees work (see figure 15). In the wake of COVID-19, flexible work arrangements have become the norm. **Prior to the pandemic, only 23% of cybersecurity professionals worked remotely or had the flexibility to choose where they worked. Today, this number has surged to 55%** (see figure 16).

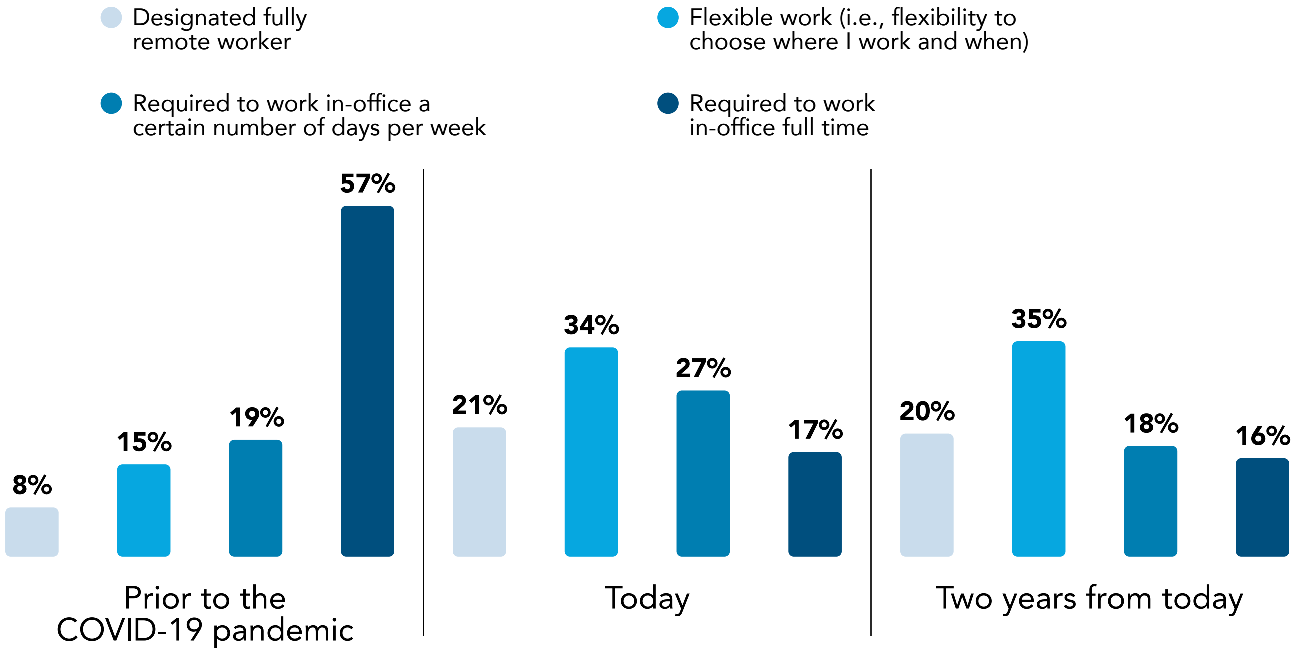
> Over half of respondents would consider switching jobs if they were no longer allowed to work remotely.

Remote work has a substantial impact on employee experience. The average EX ratings of respondents working fully remote (54.4) and flexible work (53.4) are higher than those required to be full time in the office (48.0). Some 59% said they always prefer to work remotely. Over half would consider switching jobs if they were no longer allowed to work remotely.

Suspicion around remote work is still widespread, especially among organizational leaders. 62% of non-manager cybersecurity professionals say they are more productive when working from home; this is compared to only 35% of managers who said remote staff are not as productive as onsite staff.

FIGURE 16

Which of the following best describes how you were working prior to the COVID-19 pandemic? Which best describes how you are working today? How do you think you'll be working two years from today?



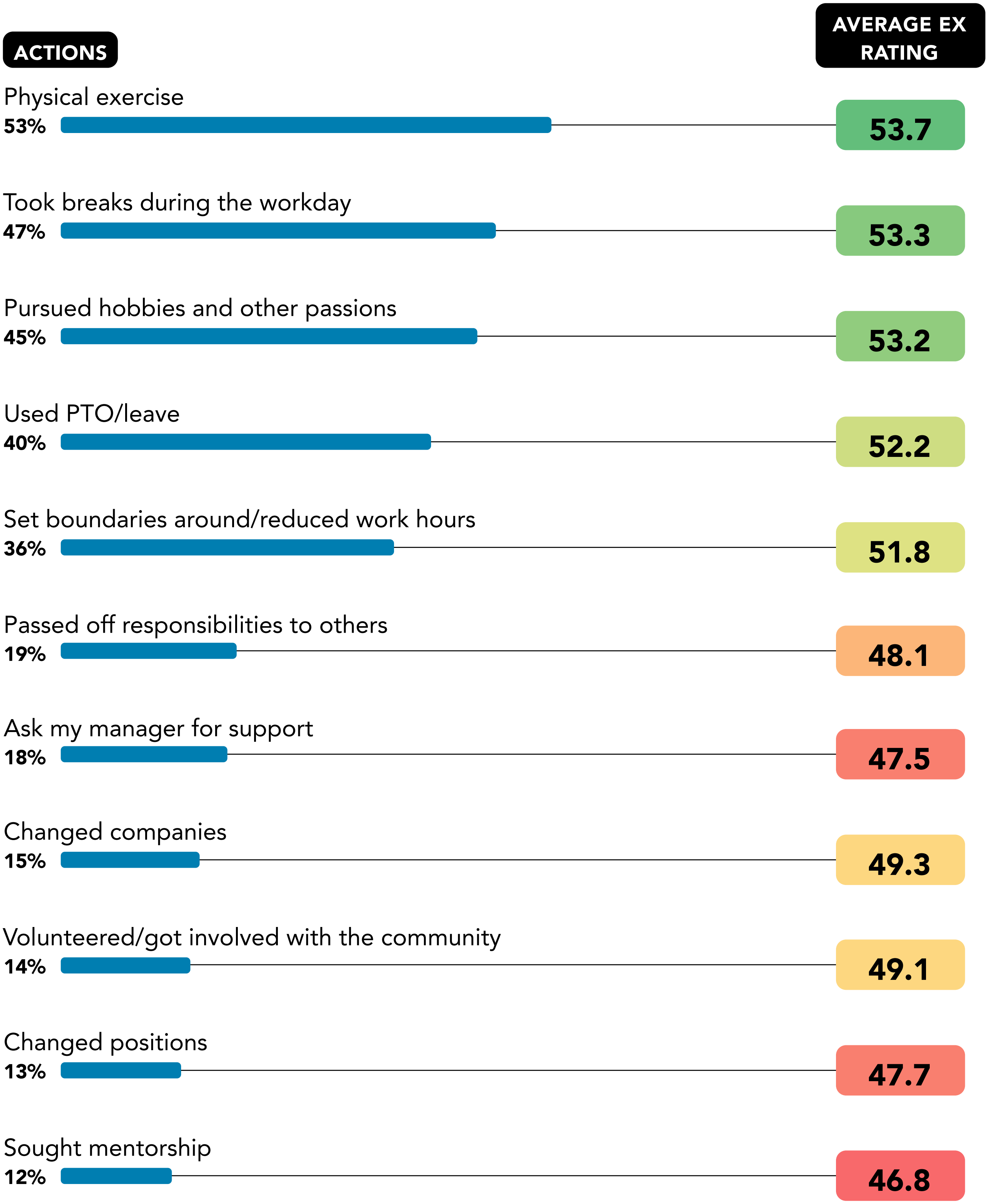
Base: 11,525 global cybersecurity professionals on cybersecurity teams

COMBATTING BURNOUT AT WORK STARTS AT HOME

The ability to avoid burnout was another key factor in EX ratings. The move to remote work has allowed people to proactively combat feelings of burnout that would otherwise weigh down their day-to-day experiences. The traditional workday is now broken up with non-work activities in between tasks, such as physical exercise and pursuing hobbies and other passions after work hours. The average EX rating for respondents using these tactics was higher than it was for those who tried to avoid burnout by changing work environments, seeking mentorship, passing responsibilities to others or changing jobs. Figure 17 shows the relative effectiveness of each activity based on the average EX score of respondents pursuing it. Remote workers engaged in the most effective activities, i.e., physical exercise and taking breaks, much more than in-office workers (see figure 18).

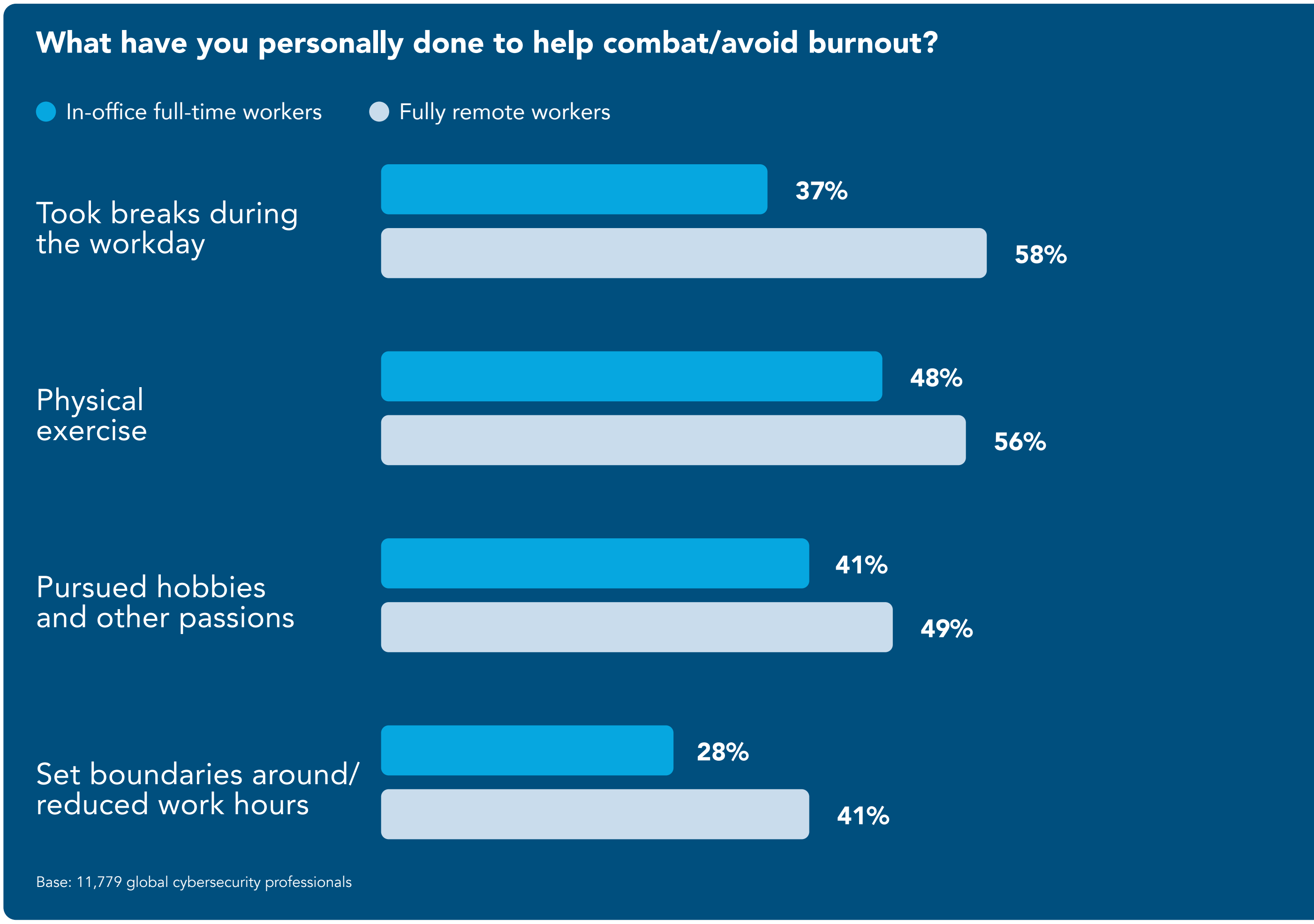
FIGURE 17

What have you personally done to help combat/avoid burnout?



Base: 11,525 global cybersecurity professionals on cybersecurity teams

FIGURE 18



What have you personally done to help combat/avoid burnout?

Base: 11,779 global cybersecurity professionals

CYBERSECURITY IS BEGINNING TO SEE A GENERATIONAL DIVIDE

Attention and attitudes toward organizational culture in the cybersecurity industry have changed considerably over the last five years. Today, many cybersecurity workers – especially younger ones – consider issues like diversity, equity and inclusion (DEI), emotional health and having a louder voice to be a greater priority (see figure 19).

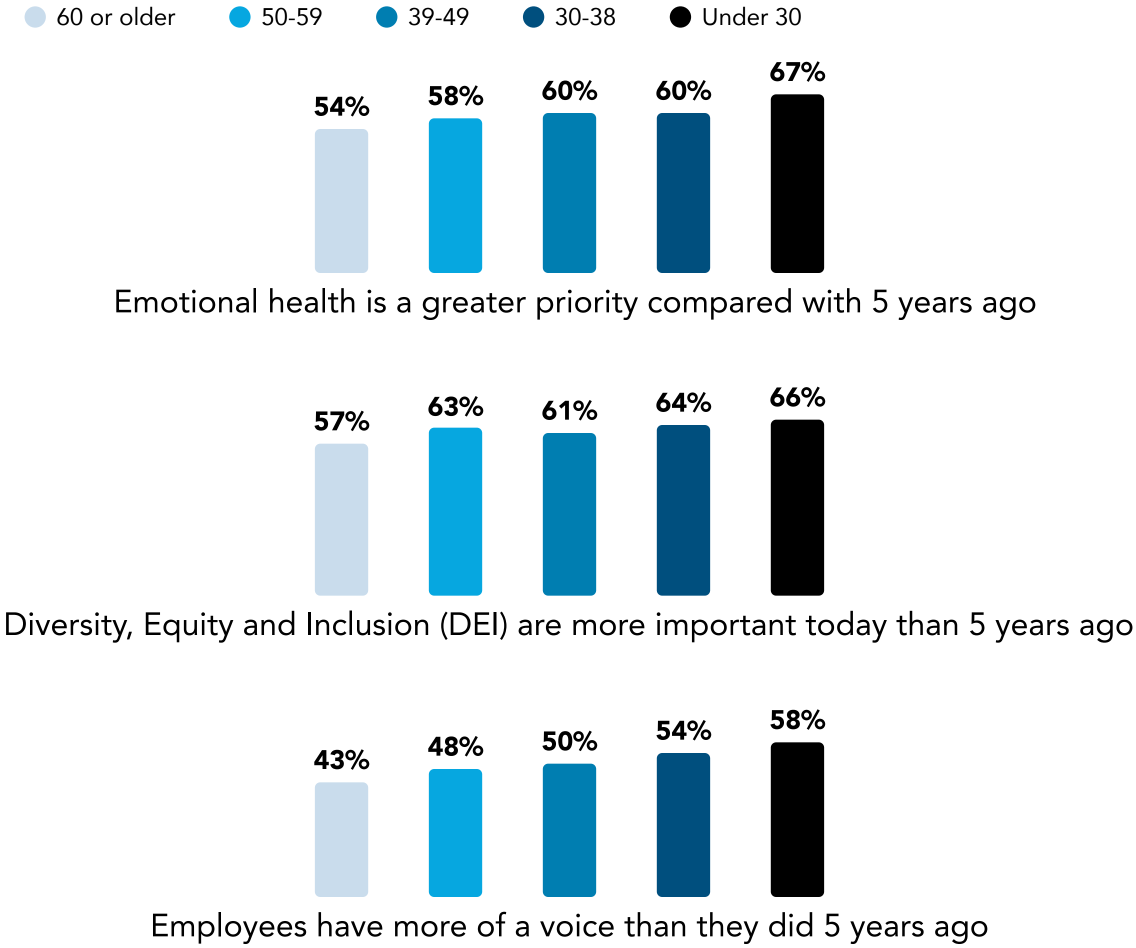
Many of these younger individuals have concerns about a perceived cultural divide between junior and senior employees. They feel that longer-tenured colleagues, their employer and the cybersecurity profession have created a "gatekeeping" culture that limits opportunity and advancement. (In the survey, "gatekeeping" was defined as an artificial or unnecessary barrier such as requirements for education, certifications or specific skills). Nearly 25% of respondents below the age of 30 considered gatekeeping and generational tensions as their top-five challenges for the next two years; this is compared to just 6% of workers who are 60 or older (see figure 20).

Findings suggest a connection between these hot-button issues and EX scores. In our survey, workers who voiced the strongest concerns in these areas had the lowest average ratings; the least concerned workers had the highest ratings (see figure 21).

FIGURE 19

To what extent do you agree with each of the following statements related to how the security industry's culture has changed in the past five years?

(Percentage showing Somewhat/Completely Agree responses)

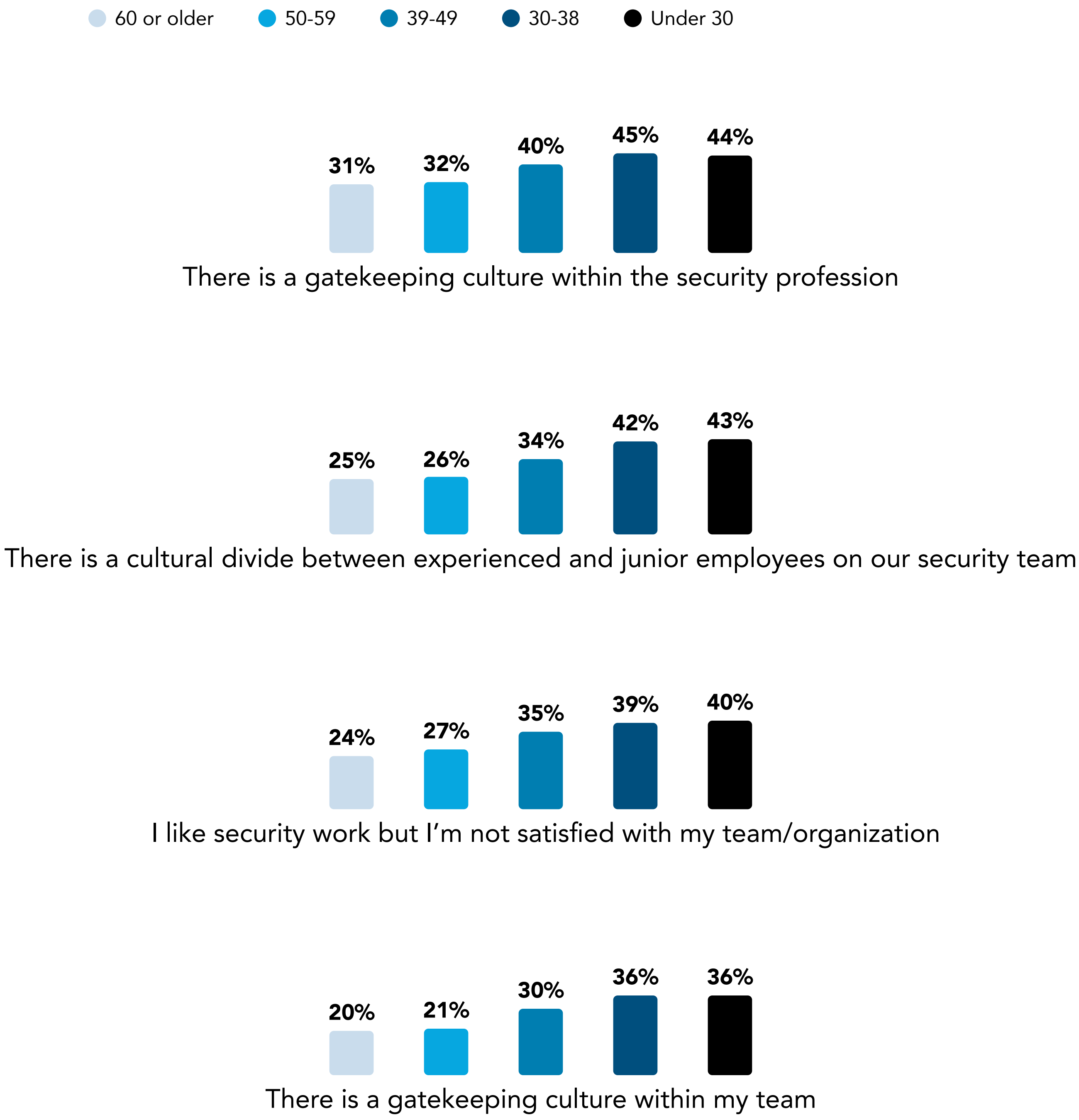


Base: 11,525 global cybersecurity professionals on cybersecurity teams

FIGURE 20

How much do you agree or disagree with the following statements about your security team's culture in general?

(Percentage showing Agree/Completely Agree responses)

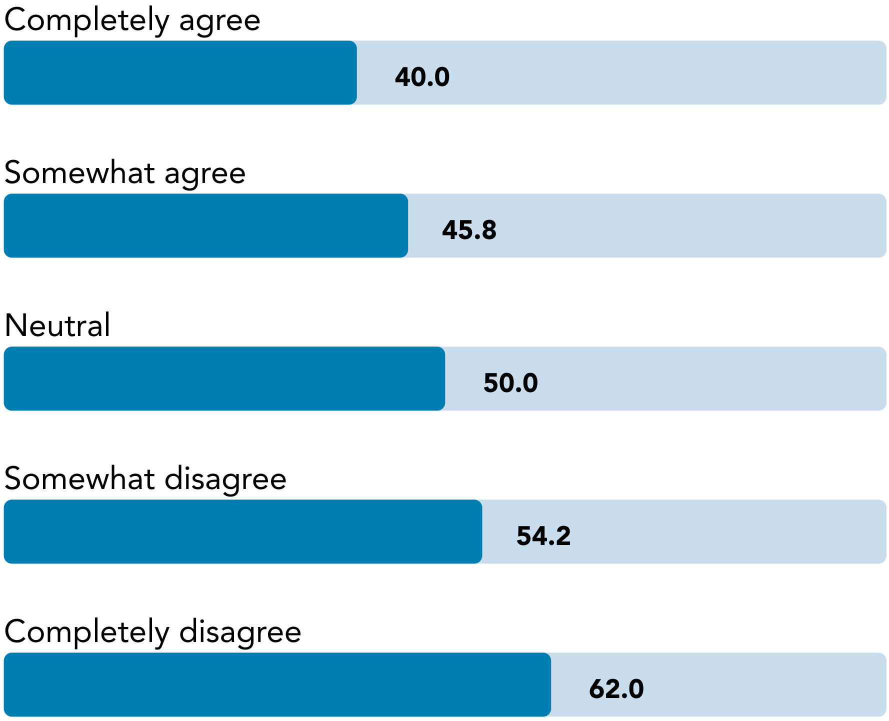


Base: 10,683-11,347 global cybersecurity professionals on cybersecurity teams

FIGURE 21

To what extent do you agree that there is a gatekeeping culture within your team?

(Showing Average EX Rating)



Base: 10,752 global cybersecurity professionals on cybersecurity teams

WHAT IT MEANS FOR ORGANIZATIONS

CYBERSECURITY TEAM CULTURE

Cybersecurity team culture is crucial to reducing employee turnover and increasing productivity. Our study found that cybersecurity personnel generally love cybersecurity work but that does not mean they are always happy in their particular organization or team. Unhappy employees are less productive and more likely to leave, costing organizations valuable time and resources to replace them. Our study found that Low EX workers were more than twice as likely to be employed at organizations with significant staffing shortages. This suggests a vicious cycle: organizations with poor EX lose staff, and this creates staffing shortages which harms EX even further. On top of retention issues, **68% of Low EX employees say that workplace culture impacts their effectiveness in responding to cybersecurity incidents.**

The key findings for organizations that are looking to prevent issues with employee experience are as follows:

- **Value your employee's voice.** Respondents not feeling as if their voices are being heard resulted in the lowest EX rating on average. Consequently, those at organizations that implemented initiatives to listen to and value the expertise of all cybersecurity staff had the highest EX rating of any organizational initiative. Therefore, it's crucial that cybersecurity leadership listens to and values the voice of all employees.
- **EX initiatives pay off.** While some initiatives to improve organizational culture have a greater impact, it's worth noting that all have a net positive effect on EX. Organizations should not discount the importance of these initiatives to improve the morale of cybersecurity teams.

- **Flexible work options have become the norm.** The pandemic changed the way in which employees expect to work. 55% of respondents currently have the flexibility to choose where they work on a daily basis, and 84% have the ability to work at home at least part time. **Over half of workers say they would consider switching jobs if they were no longer allowed to work remotely.** Organizations that are not offering flexible work arrangements are going to fall behind their competition and lose workers.
- **Prepare for a changing workforce.** Younger workers note that they are frequently feeling a cultural divide; this extends to the idea that many organizations have a "gatekeeping" culture. Organizations need to understand how the workforce at large is changing and begin to adapt. Fostering collaborative relationships between junior and senior employees can go a long way in creating a more productive and harmonious transition to a new generation of cybersecurity workers.

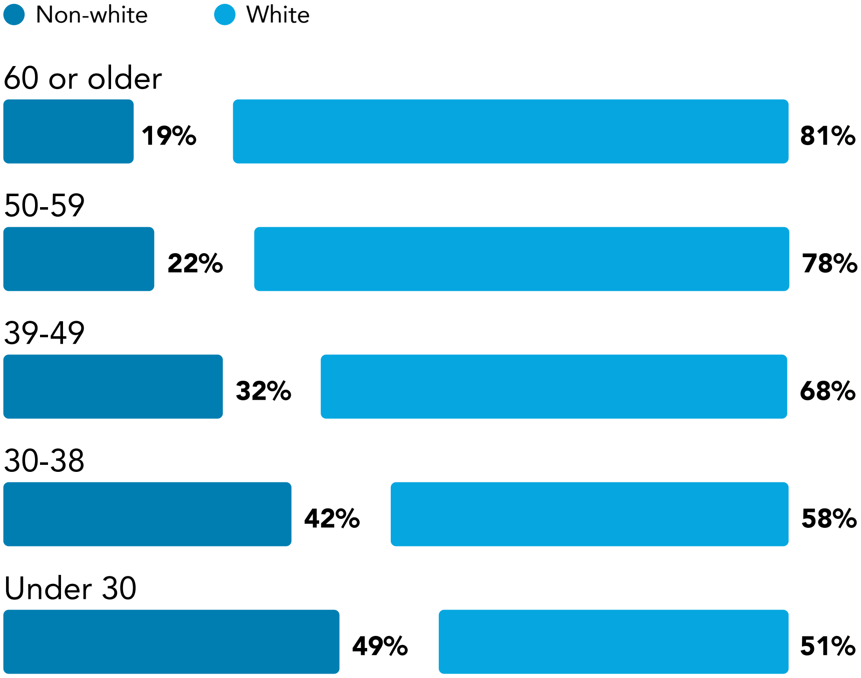
> 68% of Low EX employees say that workplace culture impacts their effectiveness in responding to cybersecurity incidents.

DIVERSITY, EQUITY AND INCLUSION

Across the world, the cybersecurity profession is rapidly changing and experiencing profound demographic shifts in age, gender, race and ethnicity. The divide between younger and older cybersecurity professionals is the greatest within DEI. This gap is the result of both generational changes in culture and in demographics themselves. For example, in our study, women accounted for 30% of global cybersecurity workers who are under the age of 30; additionally, they accounted for just 14% of those 60 or older. Dramatic shifts are happening even faster in race and ethnicity demographics (see figures 22-A and 22-B). In this study, we looked at racial and ethnic differences among cybersecurity professionals in the U.S., Canada, the United Kingdom and Ireland. In each country, the cybersecurity workforce has historically been dominated by white men, who comprise nearly 70% of the 60 or older respondents but only 40% of those under 30 (see figure 23). Cybersecurity professionals expect this demographic shift to increase even further, with 55% saying the workforce will be more diverse two years from today.

FIGURE 22-A

Age Group By Race

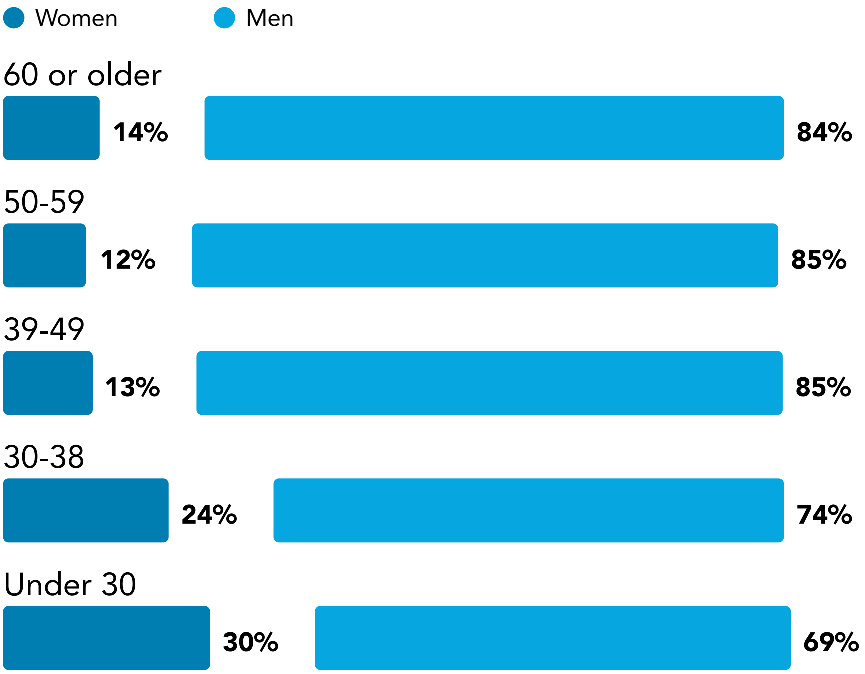


Base: 6,110 cybersecurity professionals in the United States, Canada, United Kingdom and Ireland

Note: The demographic distributions of gender, race and ethnicity should be considered a representation of the survey sample and not necessarily reflective of the cybersecurity industry as a whole.

FIGURE 22-B

Age Group by Gender

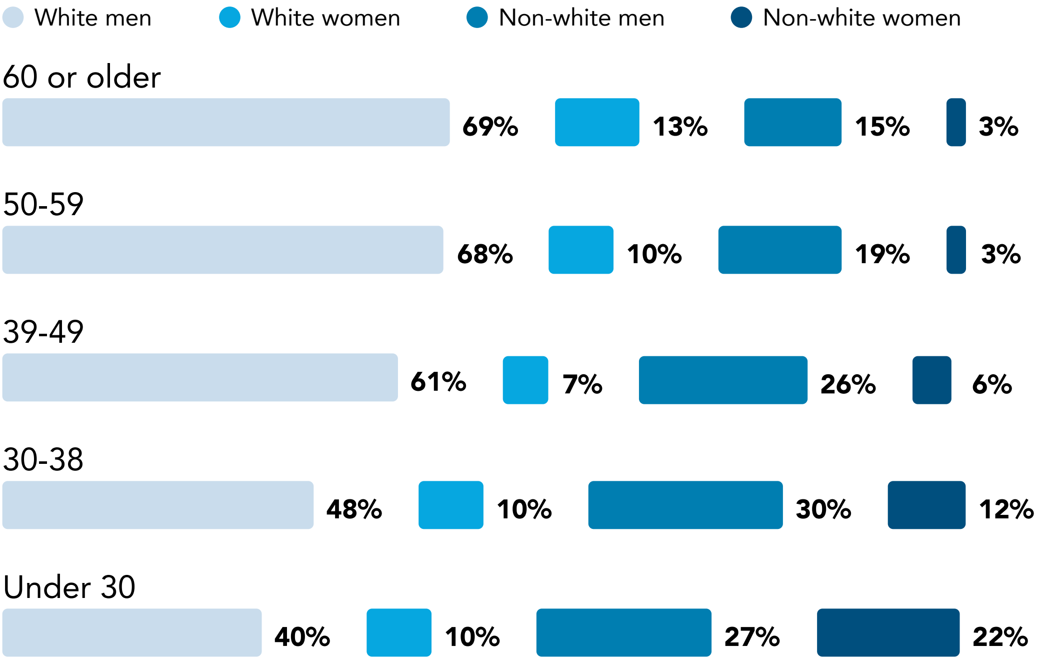


Base: 11,155 global cybersecurity professionals

Note: The demographic distributions of gender, race and ethnicity should be considered a representation of the survey sample and not necessarily reflective of the cybersecurity industry as a whole.

FIGURE 23

Age Group By Race And Gender



Base: 4,266 cybersecurity professionals in the United States, Canada, United Kingdom and Ireland

Note: The demographic distributions of gender, race and ethnicity should be considered a representation of the survey sample and not necessarily reflective of the cybersecurity industry as a whole.

Gender and race were defined in the following ways for this study:

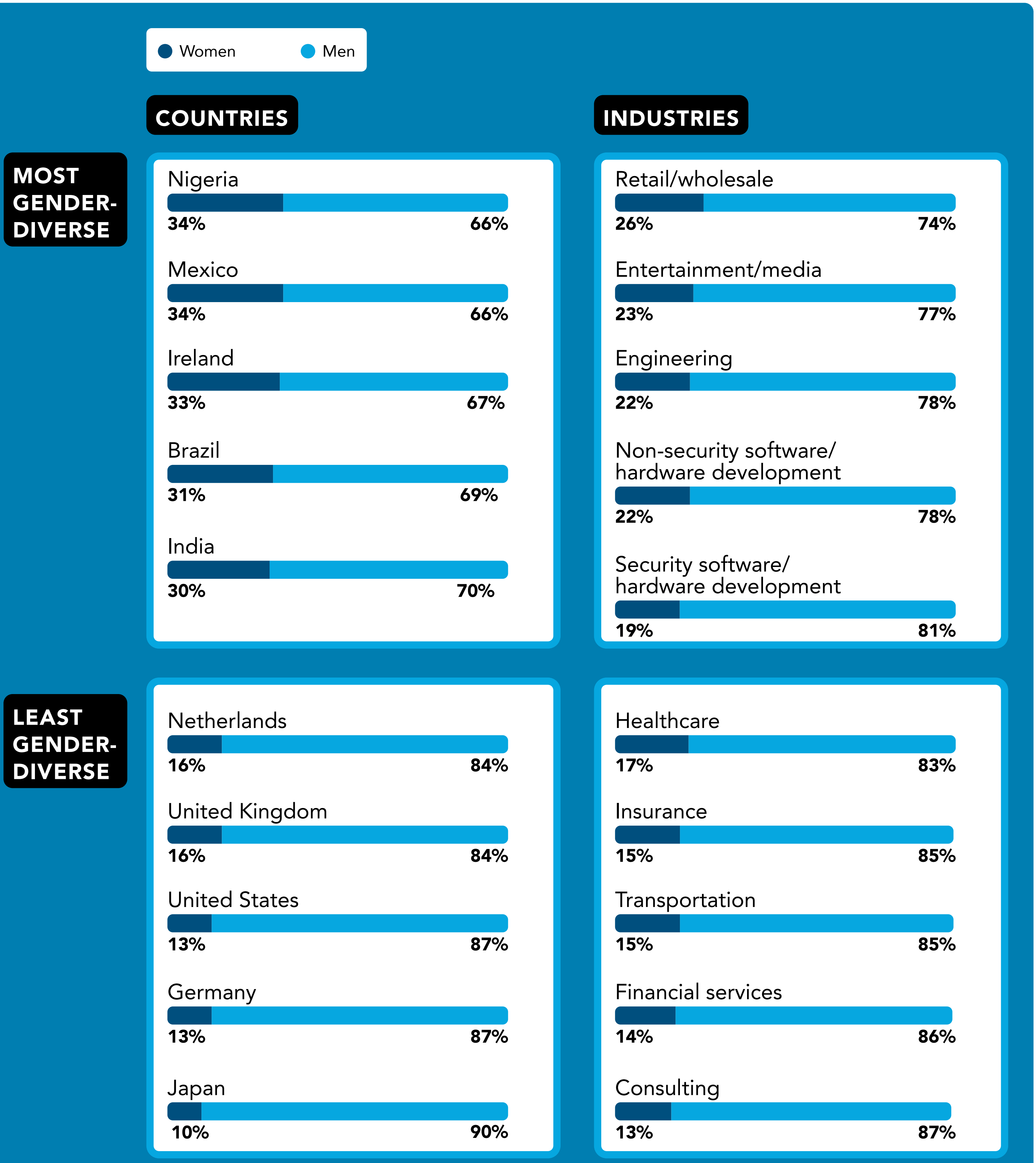
Gender: Respondents self-identified their gender as being either male, female or non-binary. Respondents who identified as non-binary represented a sample that was too small to statistically analyze, so results are not shown.

Race: Respondents were able to select any racial or ethnic group to which they felt they belonged. For the purposes of analysis, we defined "White" as any respondent who selected both "White/Caucasian" and no other racial/ethnic group. "Non-White" respondents are defined as those who selected a racial/ethnic group other than "White/Caucasian." "Non-White" respondents also include mixed-race respondents who might have also selected "White/Caucasian."

WHO'S THE BOSS? IT MAY BE CHANGING

Our survey found that higher positions are much less diverse than lower ones, e.g., only 23% of C-level cybersecurity executives identified as being non-white; this is compared with 47% of entry-level staff. It generally follows that the non-White population in cybersecurity tends to be much younger and less likely to be in executive positions.

In terms of gender, we're seeing more women, especially younger ones, holding managerial positions. In our study, women made up only 10% of C-level executives who are 50 or older, but they account for 35% of all executives in their 30s. Interestingly, women across the board remain underrepresented in advanced, non-managerial positions, where they make up only 17% of our respondent base.



Base: 11,155 global cybersecurity professionals

Note: The demographic distributions of gender, race and ethnicity should be considered a representation of the survey sample and not necessarily reflective of the cybersecurity industry as a whole.

YOUNGER WORKERS HIGHLY VALUE DEI

As demographics and cultural forces change, so do attitudes toward DEI. Younger employees placed far greater value on DEI than their older colleagues. For workers under 30, organizational diversity initiatives had the second-highest impact on EX ratings; this is behind organizations valuing and listening to their input. For those over 60, DEI had the lowest impact on EX.

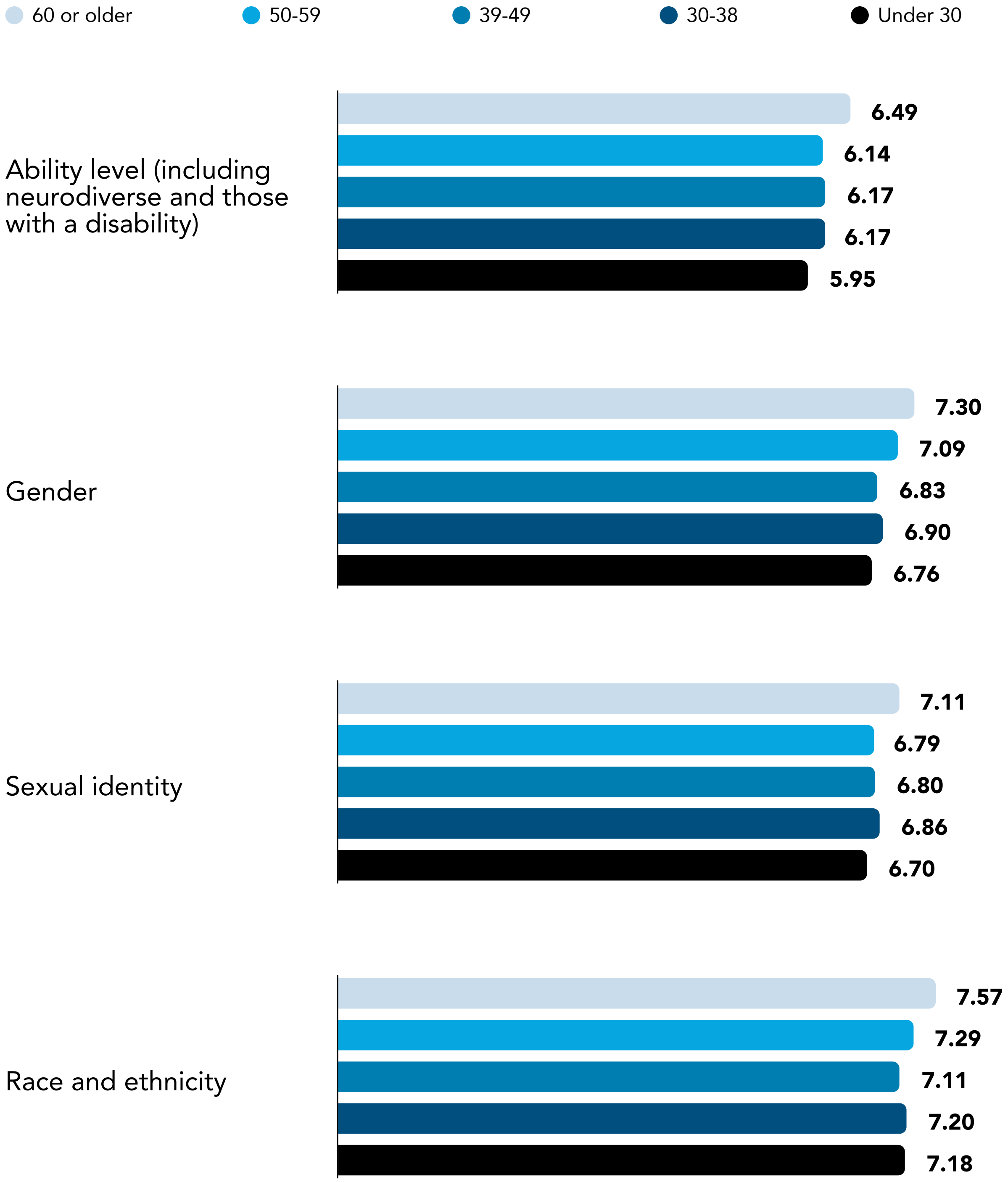
Younger employees also have different expectations. When asked to rate their organization on a scale from 1 to 10 for their efforts in diversity with age, disability, gender, sexual identity and race/ethnicity, younger employees judged their organizations much lower than their senior colleagues did in all five categories (see figure 24). Age divides are more dramatically intersected with gender and race/ethnicity. For example, younger women and non-White employees were far more likely than any demographic to agree with the following statements: "It's important that my security team is diverse" and "Diversity has contributed to my security team's success" (see figures 25 and 26). Additionally, many agreed with this statement: "I don't feel like I can be authentic and fully myself at work." It's troubling that 30% of women and 18% of non-White employees worldwide say they feel discriminated against at work.

> 30% of women and 18% of non-white employees worldwide say they feel discriminated against at work.

FIGURE 24

How would you rate your organization in terms of diversity in each of the following categories?

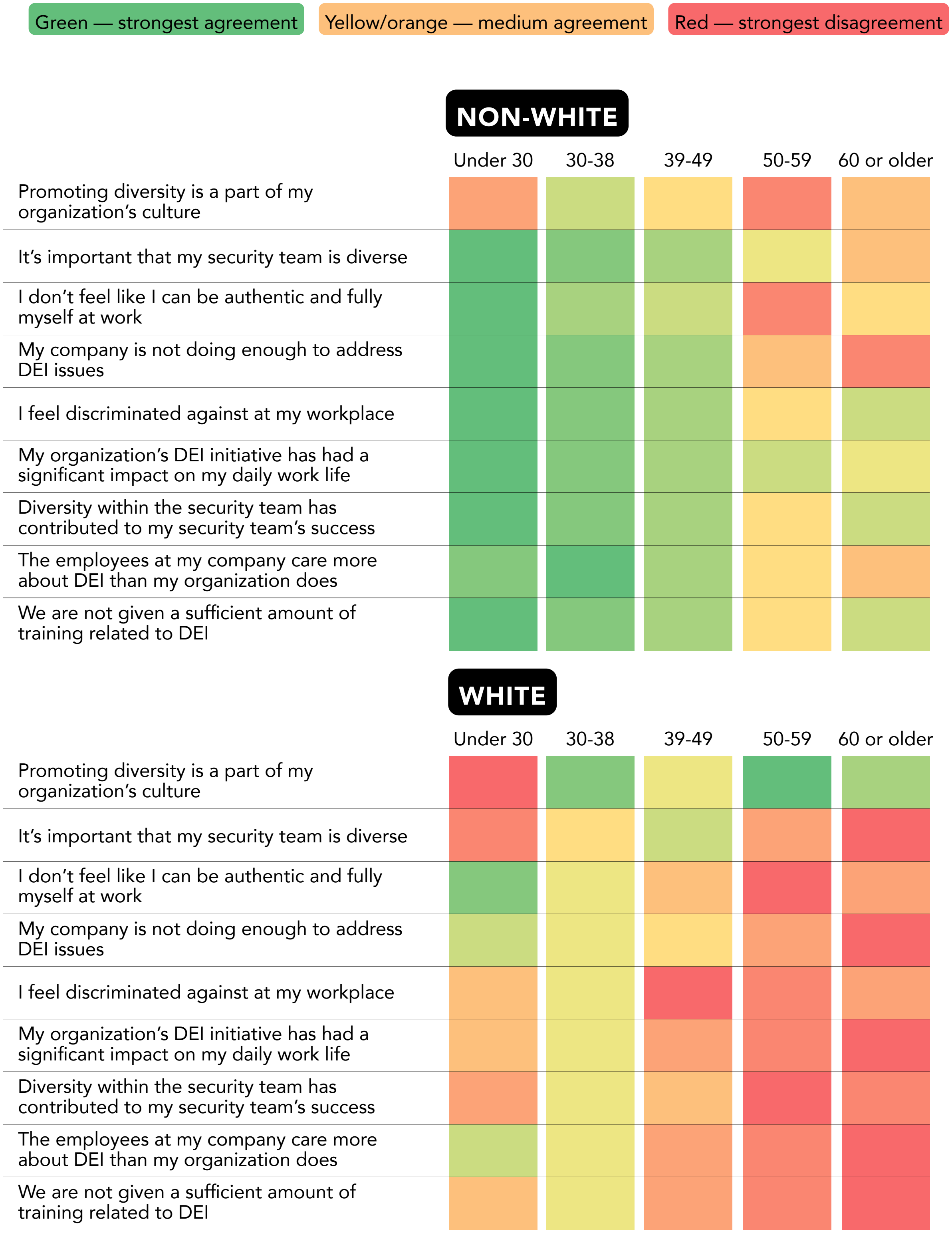
(Respondents ranked their responses on a scale of 1-10 where 1 is "not at all diverse" and 10 is "very diverse")



Base: 11,525 global cybersecurity professionals on cybersecurity teams

FIGURE 25

Who agreed most with these statements related to DEI?

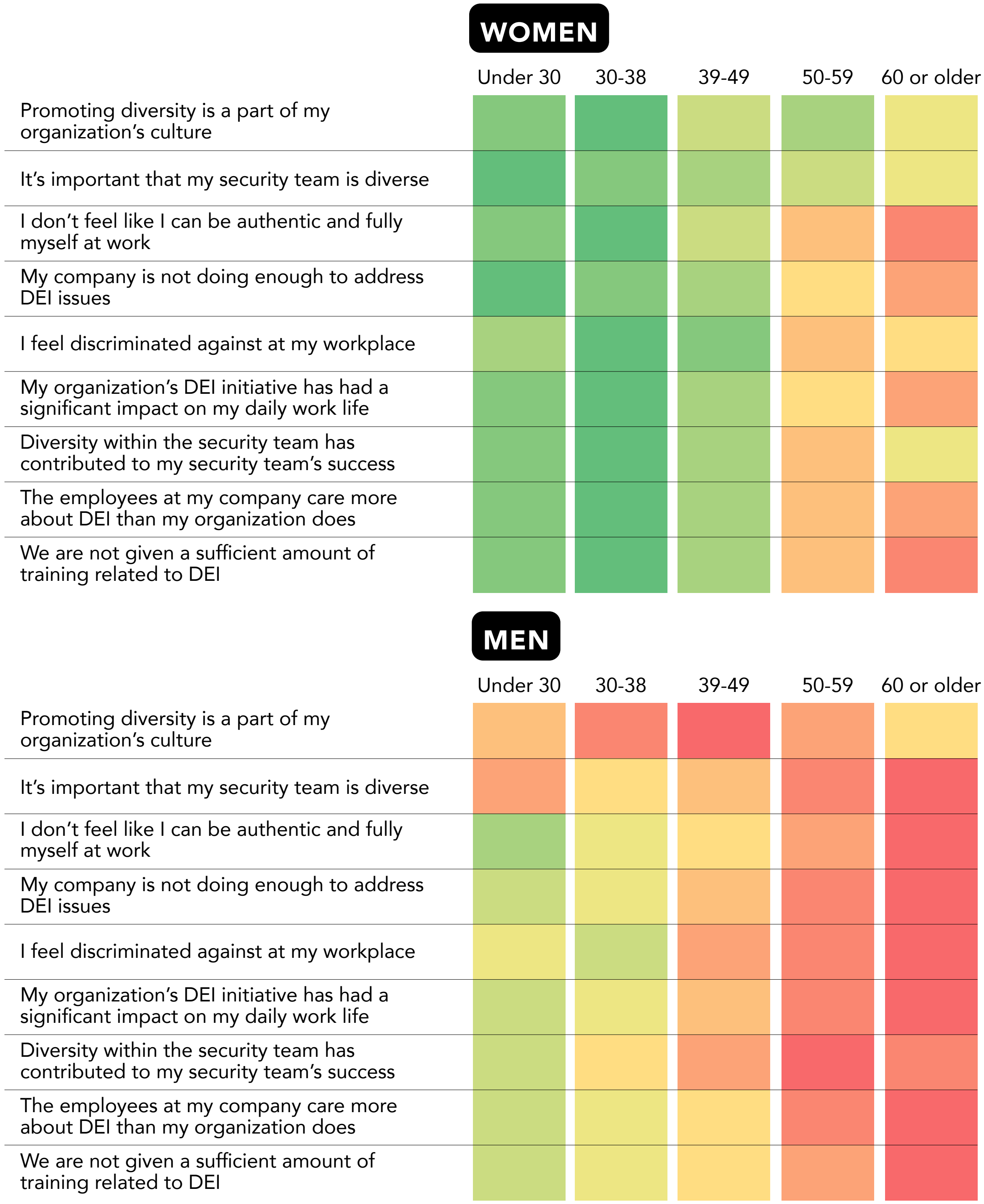


Base: 4,360 cybersecurity professionals on cybersecurity teams in the United States, Canada, United Kingdom and Ireland

FIGURE 26

Who agreed most with these statements related to DEI?

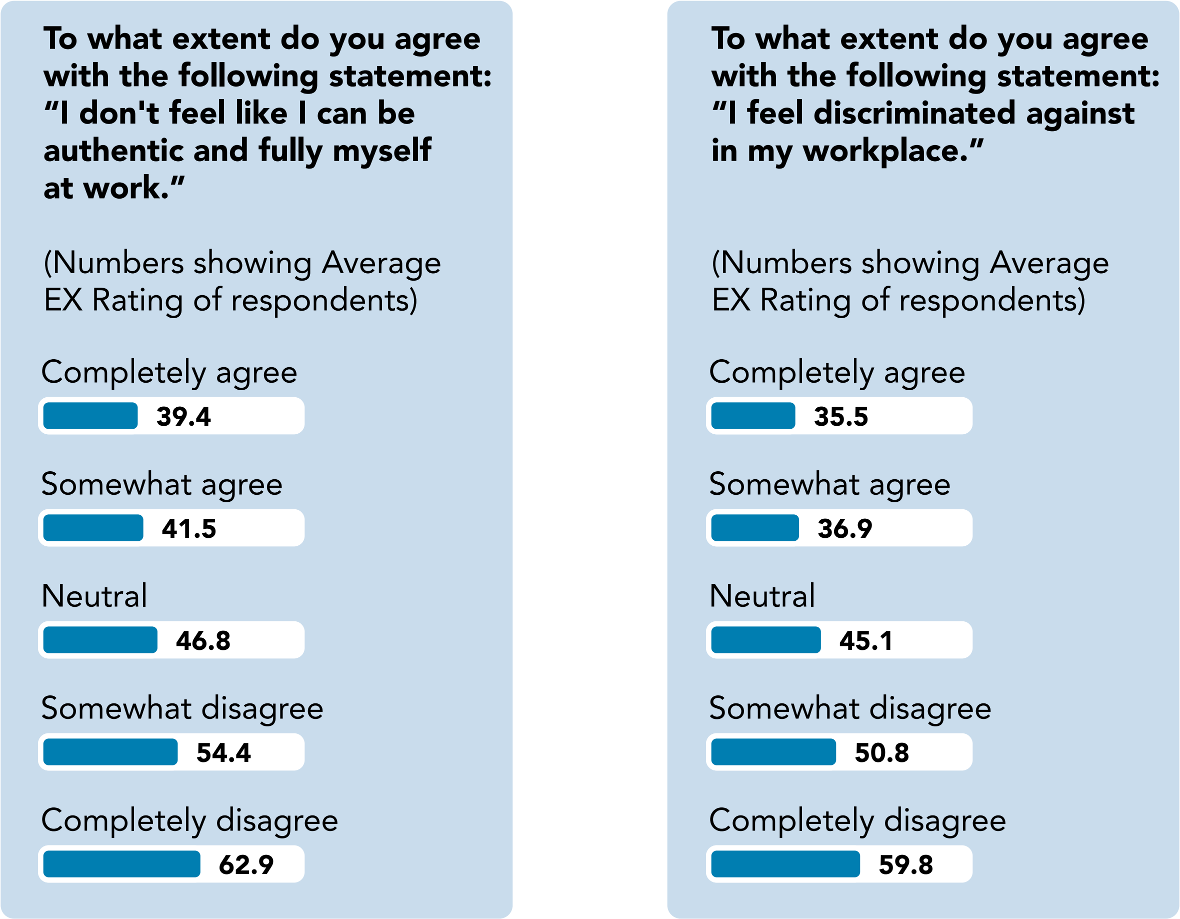
🟩 Green — strongest agreement
🟧 Yellow/orange — medium agreement
🟥 Red — strongest disagreement



Base: 11,525 global cybersecurity professionals on cybersecurity teams

DEI has a big impact on workplace culture. For many, especially young women and young people of color, this impact is focused on the employee experience. Not surprisingly, cybersecurity workers who say they feel on-the-job discrimination and the inability to be themselves at work report significantly lower EX ratings (see figure 27).

FIGURE 27



To what extent do you agree with the following statement: "I don't feel like I can be authentic and fully myself at work."

(Numbers showing Average EX Rating of respondents)

To what extent do you agree with the following statement: "I feel discriminated against in my workplace."

(Numbers showing Average EX Rating of respondents)

Base: 10,325 global cybersecurity professionals on cybersecurity teams

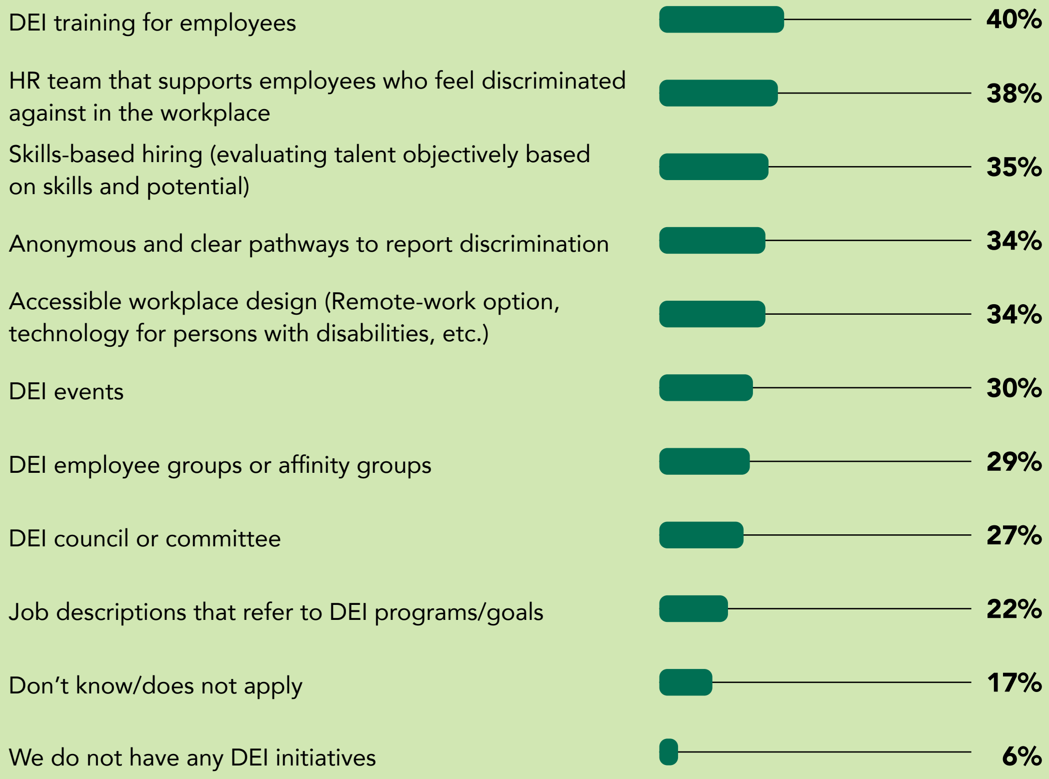
WHAT IT MEANS FOR ORGANIZATIONS

DEI

For both individual employees and organizations, DEI is an important issue. Our study found that DEI programs play a significant role in preventing or aggravating workforce shortages. Just 19% of organizations that have implemented DEI initiatives reported significant shortages of cybersecurity staff; this is compared to 34% of those who haven’t and don’t plan to do so. Our research also discovered organizations that offered more DEI initiatives had higher average EX ratings. This makes sense considering that nearly two-thirds of respondents said an inclusive environment is essential for their team’s success.

FIGURE 28

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



Base: 10,325 global cybersecurity professionals on cybersecurity teams

However, despite wide employee support, our study found that DEI-related initiatives are not widespread. Only 40% of respondents said their organizations offered employee DEI training (see figure 28). Countries in North America and Europe (except France) tended to offer more DEI initiatives; Asian countries offered the fewest.

Countries with fewer initiatives tended to have more racially and ethnically homogenous populations. Given that DEI extends beyond race and ethnicity to address gender, age, sexual identity and ability, the discrepancies are noteworthy.

DEI is an opportunity available to executive leaders. Social politics and ideologies aside, organizations should take a pragmatic look and consider the real, increasingly clear connection between DEI initiatives and cybersecurity staffing.

COUNTRIES/ECONOMIES WITH MOST DEI INITIATIVES:

1	United States
2	Ireland
3	Sweden
4	United Kingdom
5	Canada

COUNTRIES/ECONOMIES WITH FEWEST DEI INITIATIVES

1	Hong Kong
2	Japan
3	South Korea
4	France
5	China

Base: 10,325 global cybersecurity professionals on cybersecurity teams

Career Pathways

As corporate cybersecurity culture evolves to define the employee experience, career pathways are being carved out by the next generation. New trends and perspectives are emerging, i.e., evolution is motivating people and organizations to value education, certifications and practical skills differently than they have in the past.

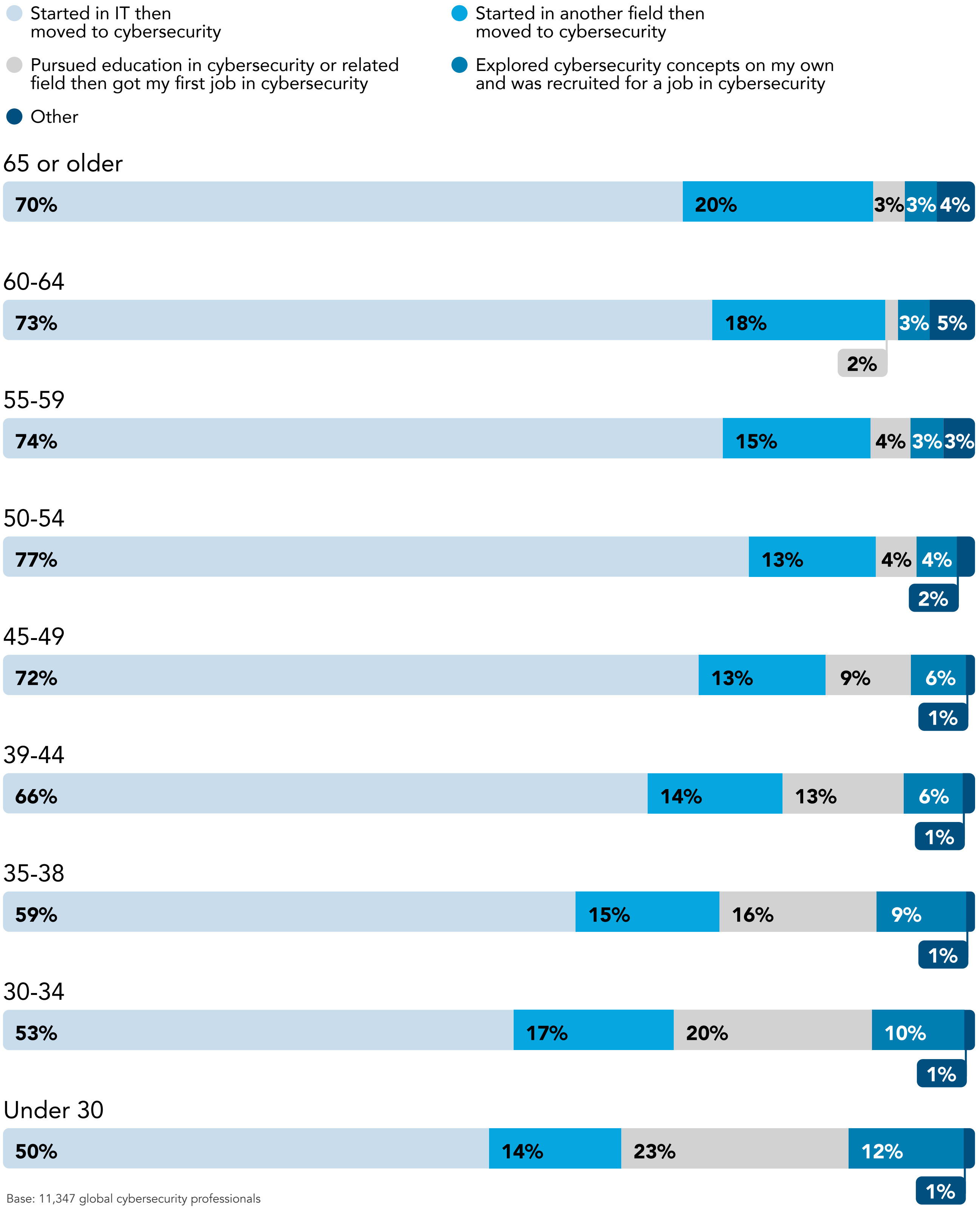
We surveyed respondents from all walks of life who are using their own education (both institutional and personal) and professional experience (both in and out of IT) as starting blocks to break into the industry. Here's what we learned:

- **For younger workers, more roads lead to cybersecurity.** Nearly half of respondents under the age of 30 move into cybersecurity from a career outside of IT. Younger professionals are more likely to use their education in cybersecurity or a related field (23%) as a stepping stone to either enter the profession or move from a totally different field (13%) outside the IT or cybersecurity landscape. Some are even recruited after their own self-education within cybersecurity (12%). As respondents approach ages 50 to 54, we observed a peak in the number of employees who have used a career in IT as their pathway into the field (74%), demonstrating that this very popular practice is no longer the primary source for recruiting younger cybersecurity talent (see figure 29).

> The primary driver for earning certifications in the future is fueled by a need to improve skills for a specific position (64%).

FIGURE 29

Which of the following best describes your pathway into a job in cybersecurity?

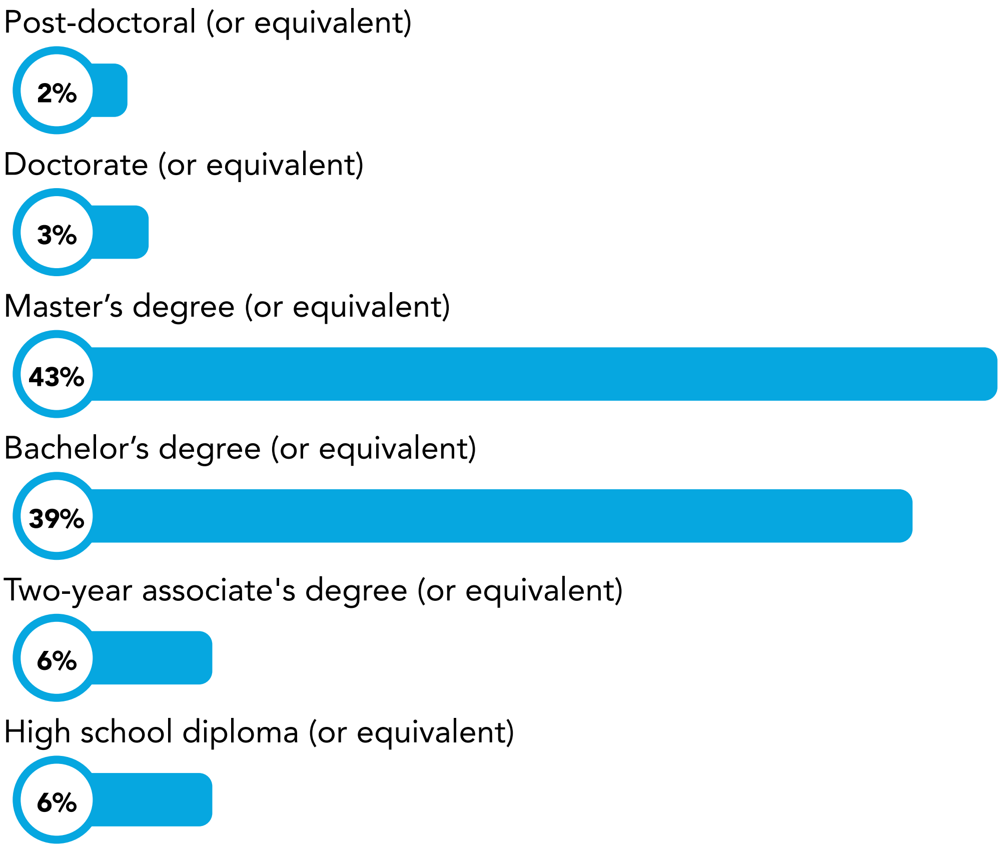


Base: 11,347 global cybersecurity professionals

- **Cybersecurity professionals are highly educated.** Out of those surveyed, 39% have attained a bachelor's degree as their highest form of education, 43% have earned a master's degree, and 5% have attained a doctorate (3%) or post-doctoral (2%) degree (see figure 30).

FIGURE 30

What is the highest level of education you have completed?

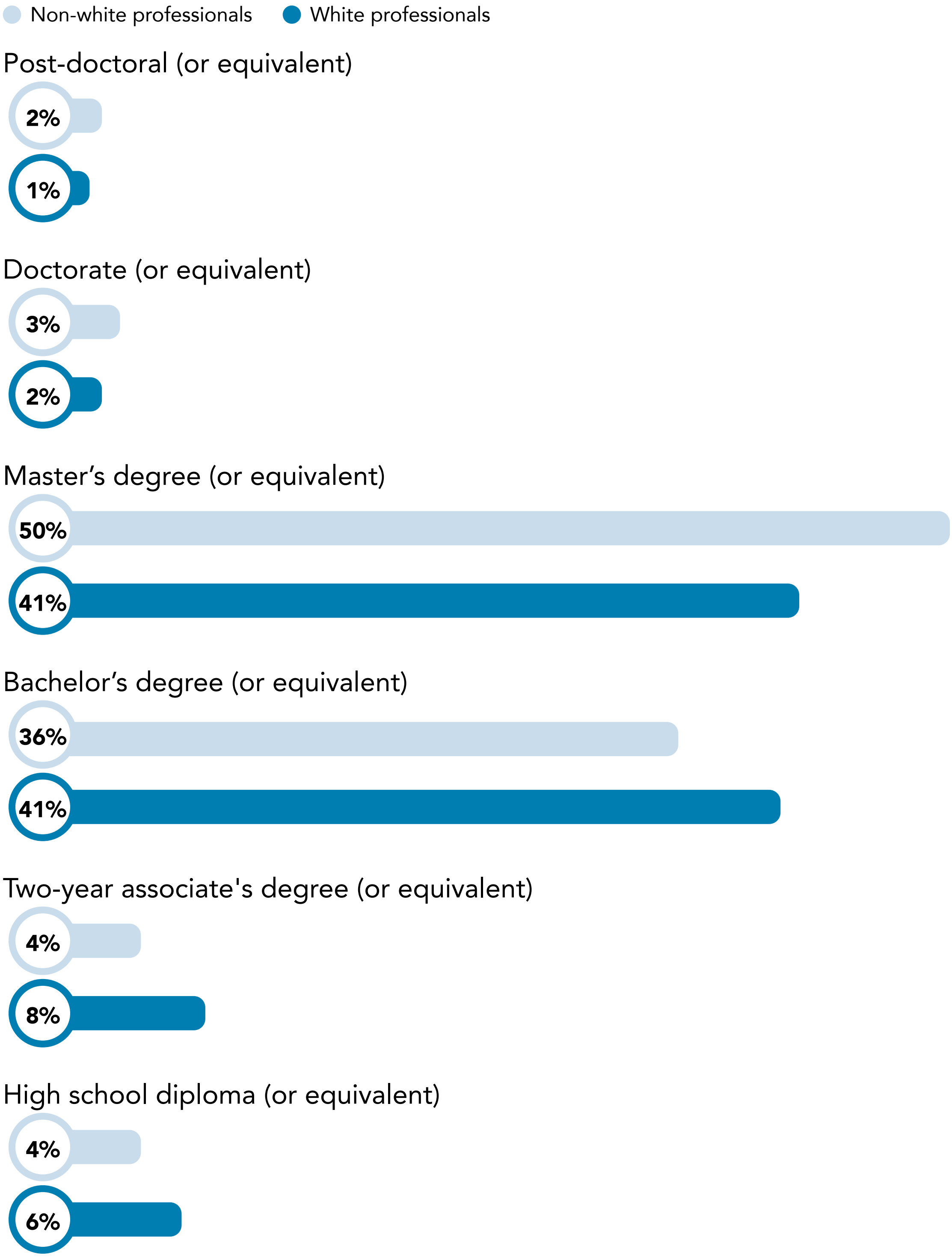


Base: 11,779 global cybersecurity professionals

As we look deeper into the different perspectives and demographics present within our research, we can extract some interesting findings. For example, women in cybersecurity are more likely to hold master's degrees than men (49% compared with 42%). In addition, 55% of non-White cybersecurity professionals hold a master's, doctorate or post-doctoral degree; this is compared to 44% of White respondents (see figures 31-A and 31-B).

FIGURE 31-A

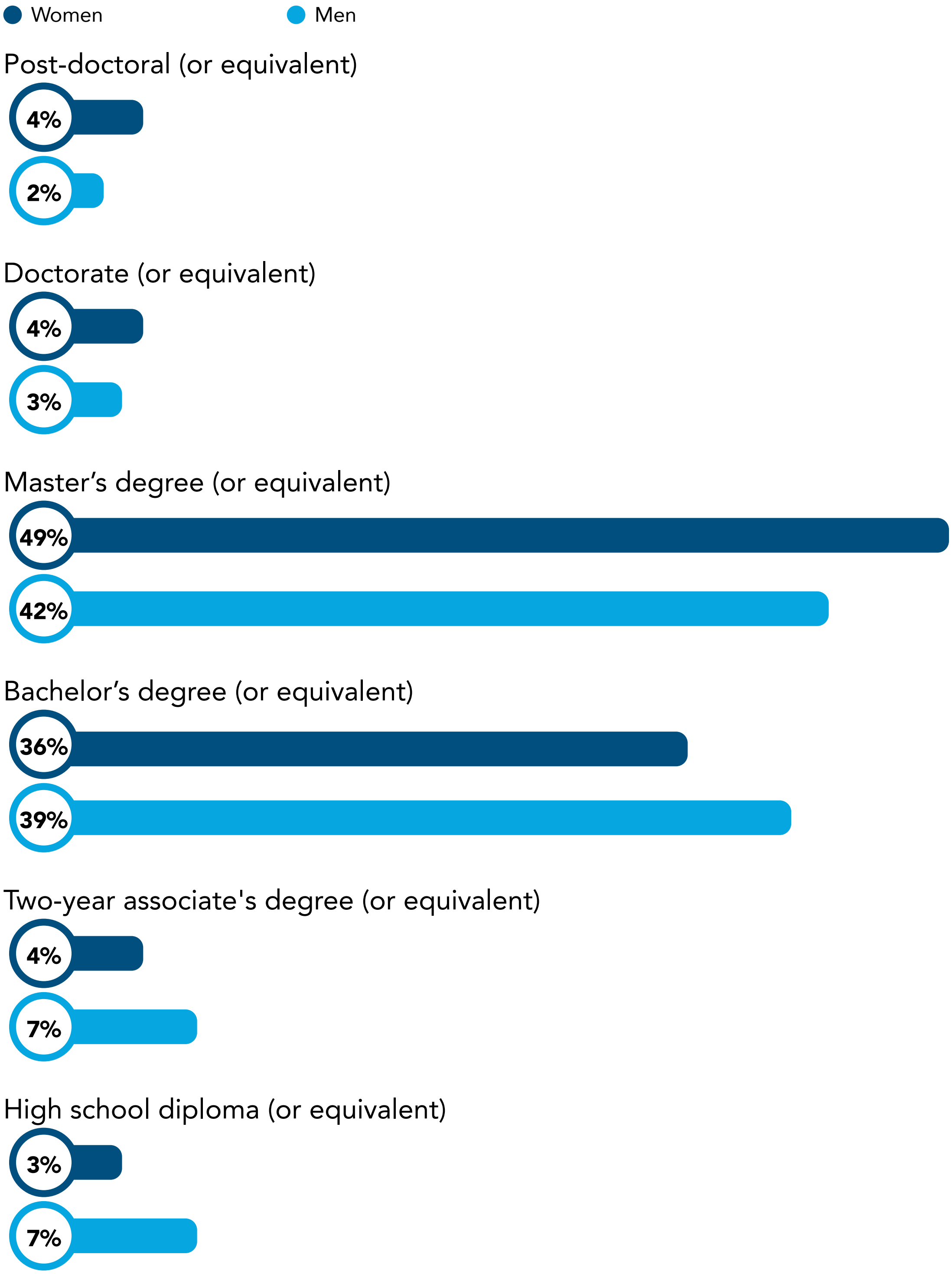
What is the highest level of education you have completed?



6,110 cybersecurity professionals on cybersecurity teams in the United States, Canada, United Kingdom and Ireland

FIGURE 31-B

What is the highest level of education you have completed?

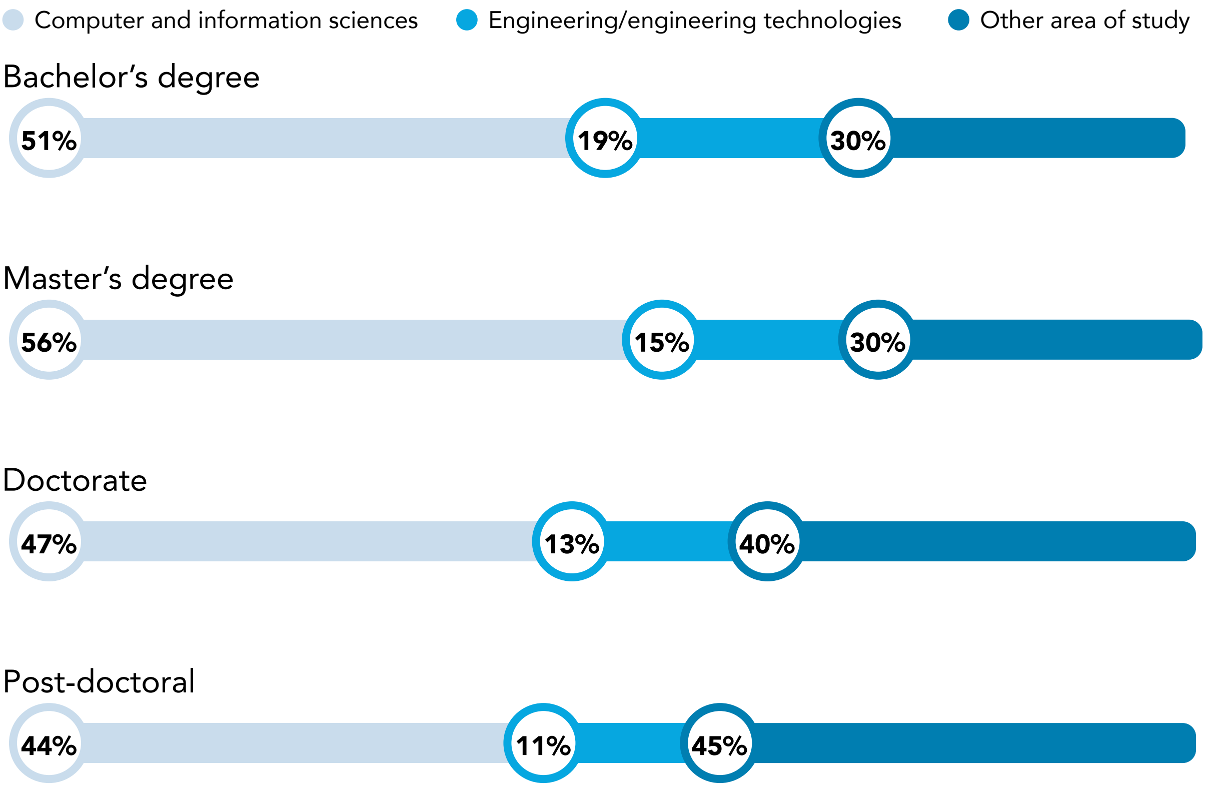


Base: 11,155 global cybersecurity professionals

Most of the surveyed cybersecurity professionals focused their education on computer and information sciences, with 51% of bachelor's degrees and 56% of master's degrees having been earned within this field. Engineering was the next most common background, with 19% of bachelor's degrees and 15% of master's degrees coming from engineering. The remaining 30% are comprised of a mix of business, communications, social sciences, mathematics, economics, biological and biomedical sciences and other degrees outside of IT (see figure 32).

FIGURE 32

Which of the following best describes the focus of your education?



Base: 281-10,302 global cybersecurity professionals who hold these degrees

- **For new hires, experience and practical skills are growing in importance**. From 2021 to 2022, practical skills and experience have grown into being more important qualifications for those considering employment in the cybersecurity profession. In particular, more emphasis is being placed on relevant IT work experience (29% to 35%), strong problem-solving abilities (38% to 44%) and relevant cybersecurity work experience (31% to 35%). The ubiquitous importance of certifications was less prioritized this year (29% vs. 32%), as were cybersecurity qualifications or trainings (17% vs. 23%), graduate degrees (10% vs. 13%) and undergraduate degrees (10% vs. 14%) (see figure 33).

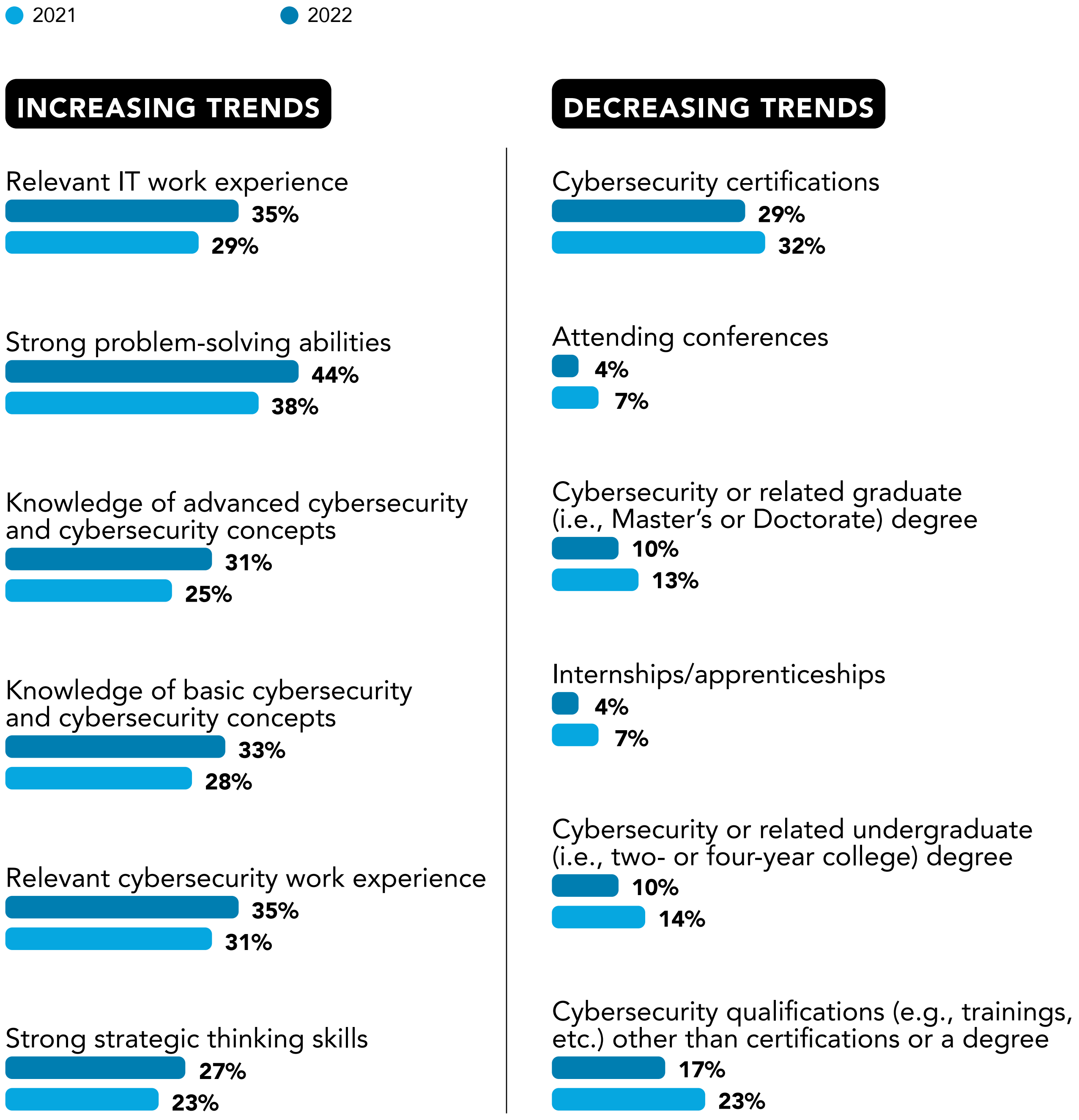
  Interestingly, when we look at how different genders responded to this data, we can see that women value cybersecurity degrees more than men, and men place significantly more emphasis on practical skills like problem-solving and communication. This is in line with the fact that a greater percentage of women in the cybersecurity field hold degrees in higher education (see figure 31-B).

> From 2021 to 2022, practical skills and experience have grown into being more important qualifications for those considering employment in the cybersecurity profession.

FIGURE 33

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

(Showing top 6 increasing and decreasing trends)



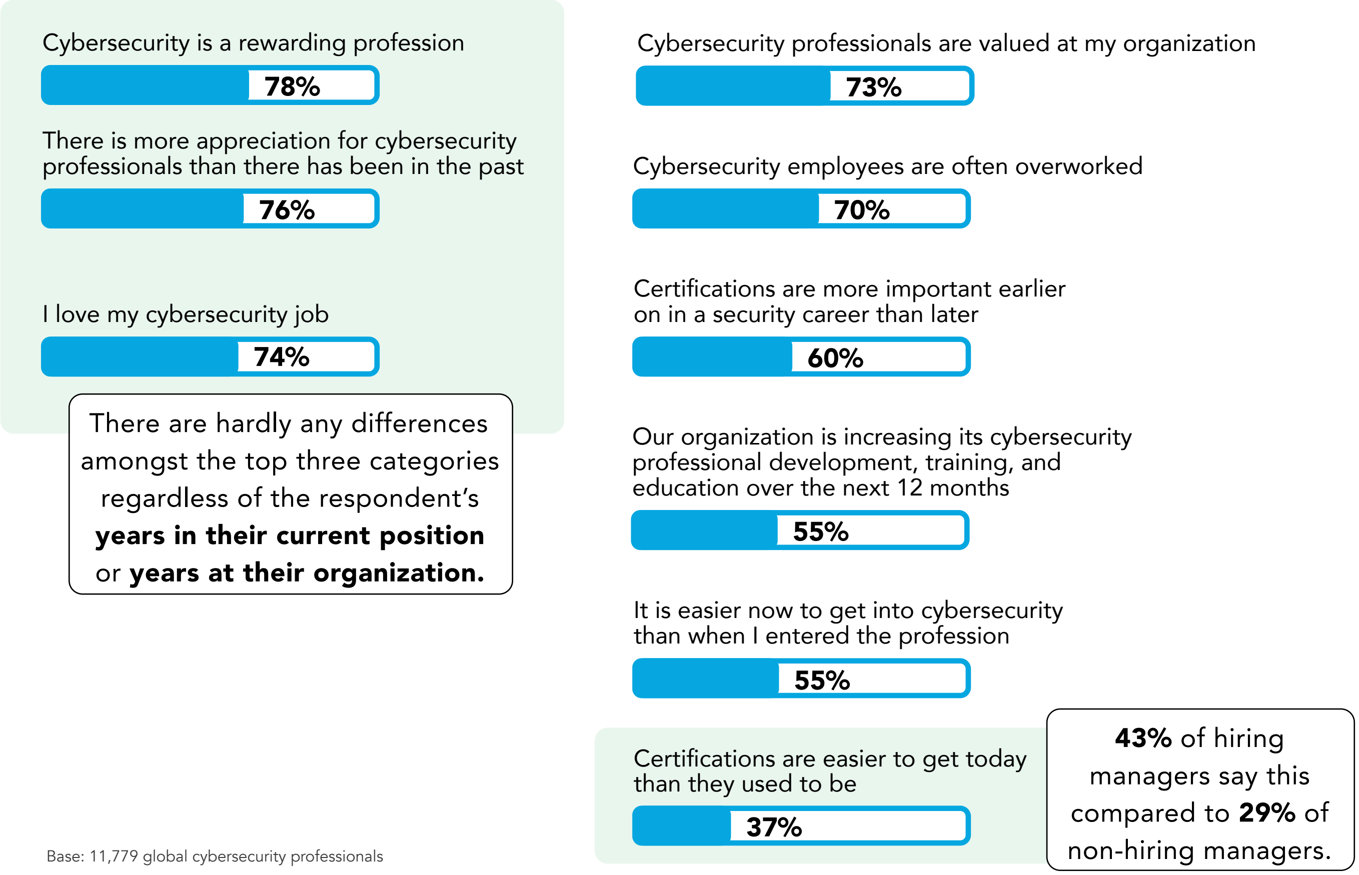
Base: 11,779 global cybersecurity professionals

- **Despite a high level of work, cybersecurity is a rewarding profession that is growing in recognition.** When all is said and done, cybersecurity professionals feel passionate about their work. While they often feel overworked (70%), an even higher number stated that it is a rewarding profession (78%). 76% agree that there is more appreciation for it than in the past, with another 74% of respondents saying that they love their job. It's important to note that there are hardly any differences within these categories when we compared respondents in their current positions with those who were at the same organization **for a year or less**, vs. those who were with a company **for more than two years**. This suggests that cybersecurity professionals are passionate about their work, regardless of age or experience (see figure 34).

FIGURE 34

To what extent do you agree or disagree with the following statements about the security profession?

(Showing Somewhat/Completely Agree responses)



There are hardly any differences amongst the top three categories regardless of the respondent's **years in their current position** or **years at their organization.**

43% of hiring managers say this compared to **29%** of non-hiring managers.

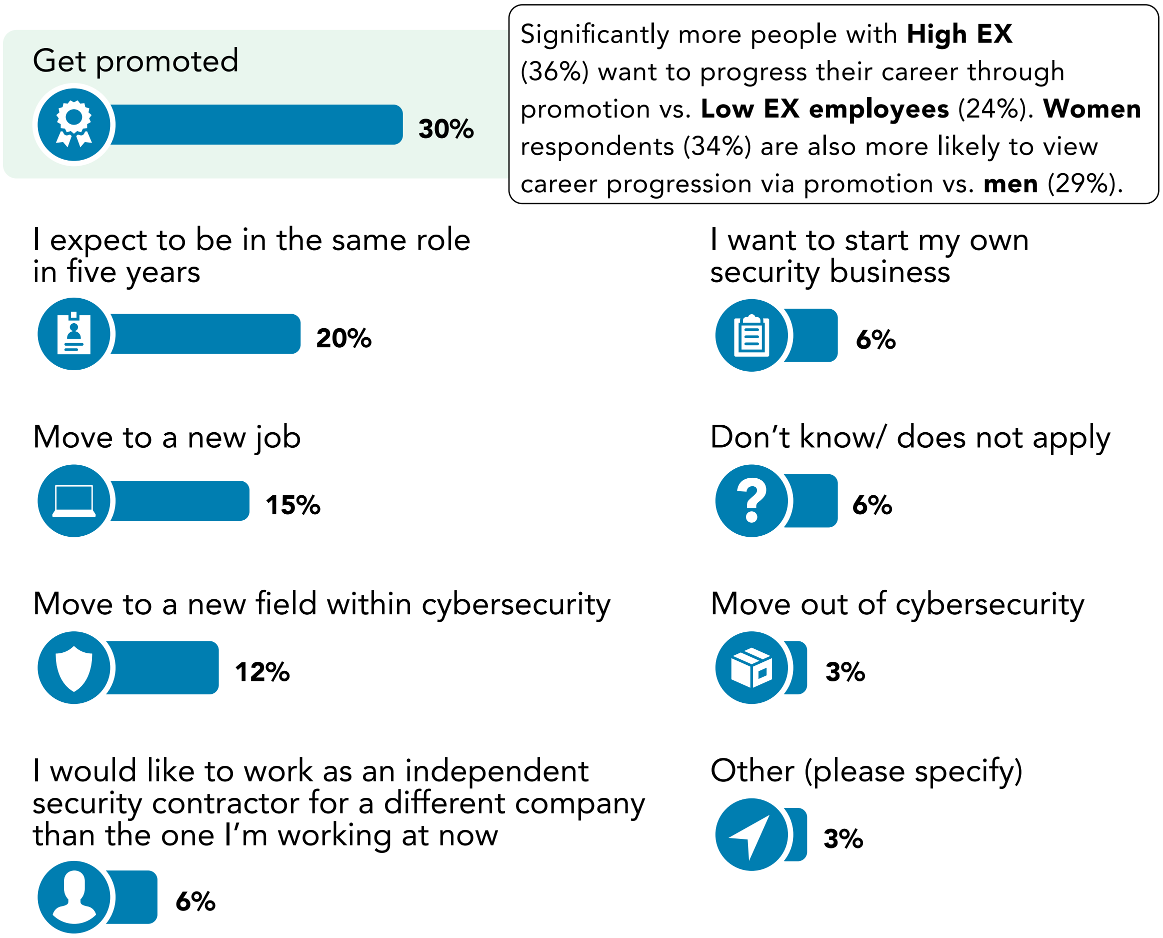
Base: 11,779 global cybersecurity professionals

- **Twice as many people view internal promotion as their next career milestone vs. changing jobs.** Despite cybersecurity's high turnover in 2022, respondents indicated that they would generally prefer internal promotion (30%) over getting a new job (15%); this is compared to moving to a new field within cybersecurity (12%), becoming an independent contractor (6%) or starting a business (6%) (see figure 35).

  When we look deeper, those who seek promotion are also more likely to be happier at their jobs. 36% of those with High EX want to progress their career through internal promotion vs. just 24% with Low EX. In addition, women (34%) are more likely to view promotion as their next career step, compared to men (29%).

FIGURE 35

How do you see your cybersecurity career progressing in the next five years?



Significantly more people with **High EX** (36%) want to progress their career through promotion vs. **Low EX employees** (24%). **Women** respondents (34%) are also more likely to view career progression via promotion vs. **men** (29%).

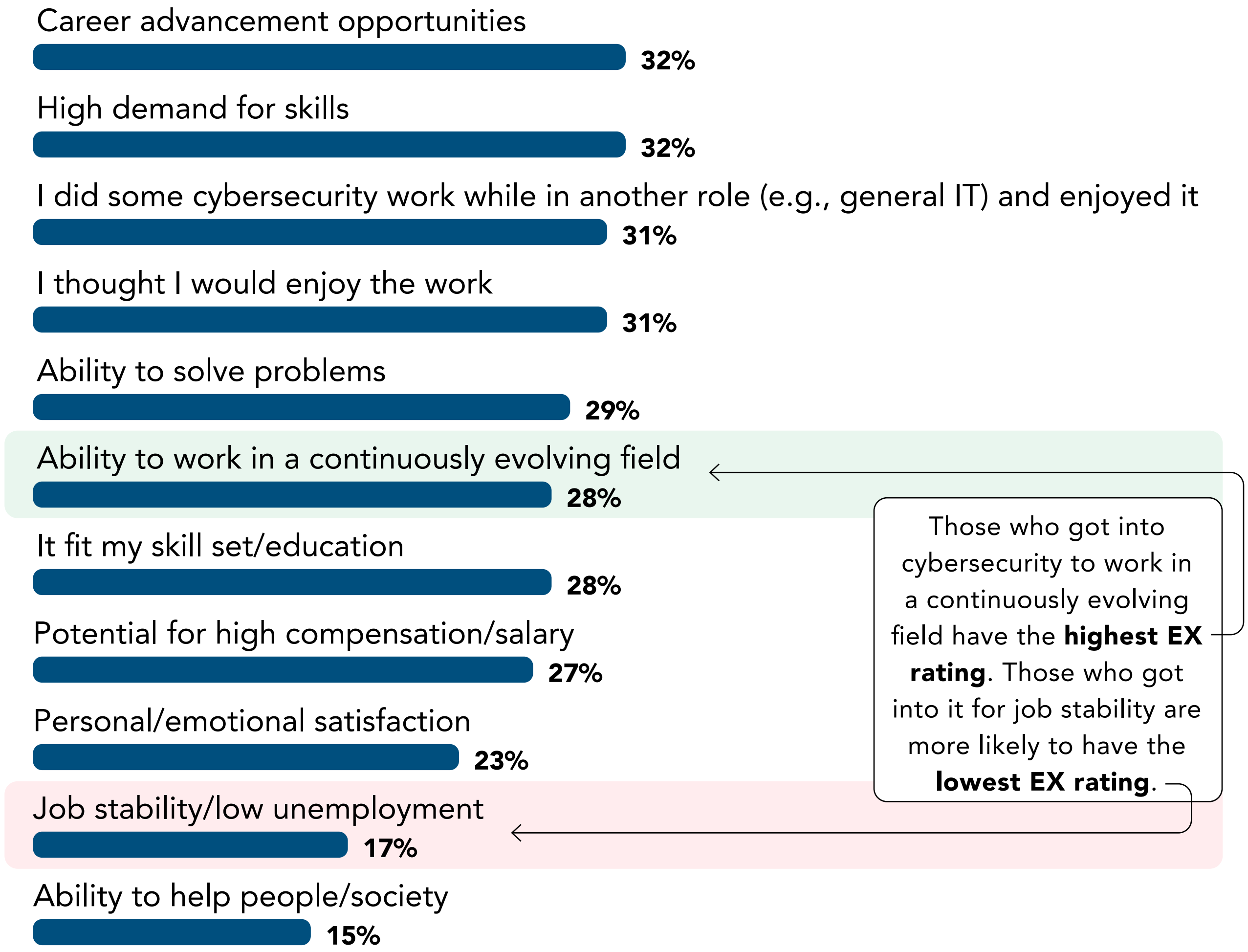
Base: 11,779 global cybersecurity professionals

- **Those who enter the field to be challenged by an evolving landscape often have a better experience.** Motivations to enter the cybersecurity field play a big role in the satisfaction that people get out of it. Although the cybersecurity field is a challenging profession that can lead to lots of work, those who dive in headfirst looking for a continuously evolving landscape displayed the highest EX rating; this is compared to those who selected any other reason. Consequently, those who chose the profession simply for "job stability" had the lowest EX rating on average (see figure 36).

FIGURE 36

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

(Showing respondents' top three responses)



Those who got into cybersecurity to work in a continuously evolving field have the **highest EX rating**. Those who got into it for job stability are more likely to have the **lowest EX rating**.

Base: 11,779 global cybersecurity professionals

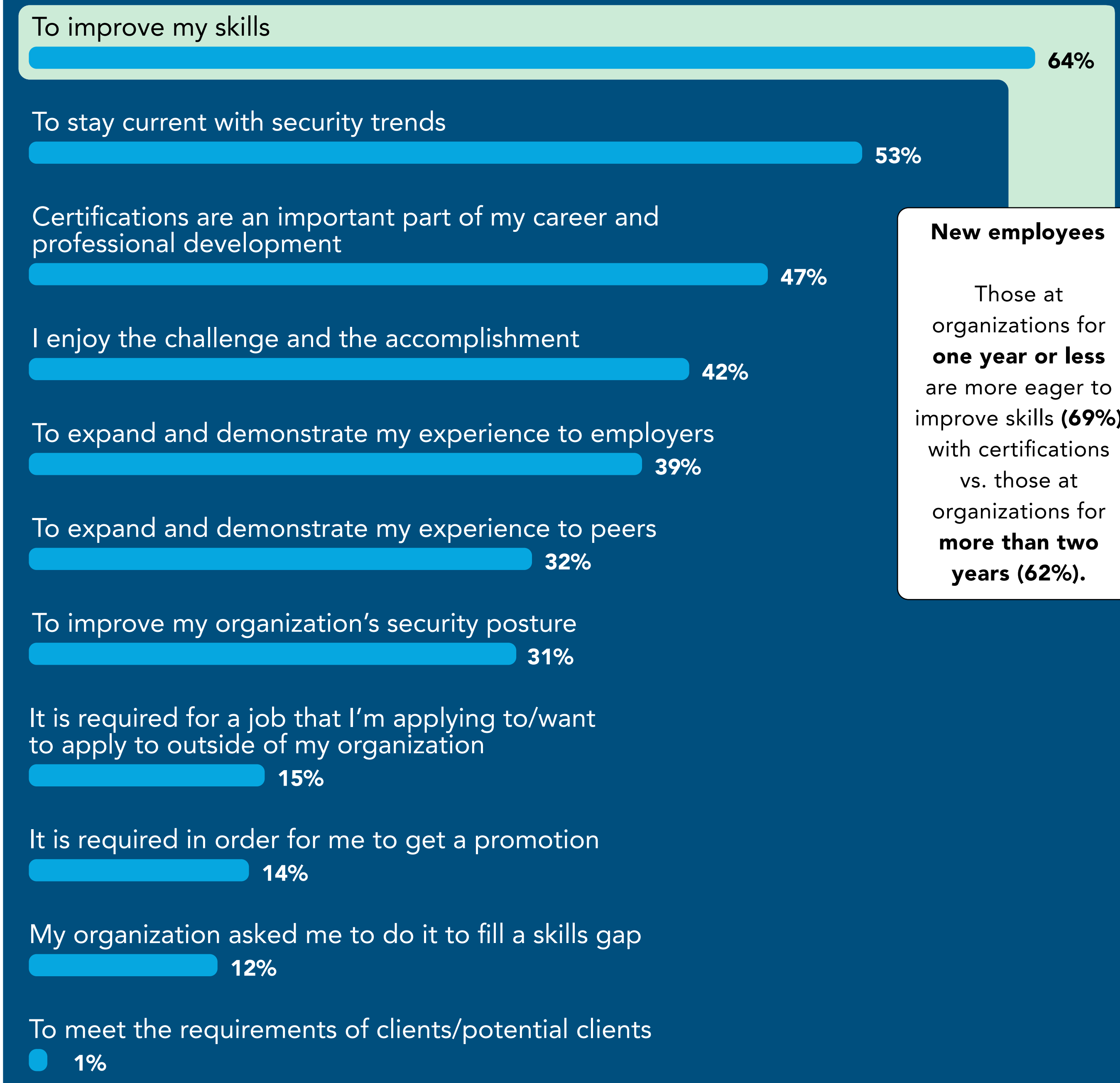
CERTIFICATIONS

- **Certifications are evolving as an instrument for skills growth, as opposed to a career launchpad.** 96% of respondents within our sample have earned at least one type of certification. In the past, most cybersecurity professionals chose certifications as a means of career progression and professional development (53%). The primary driver for earning certifications in the future is fueled by a need to improve their skills (64%) and stay current with cybersecurity trends (53%). Cybersecurity professionals are now tailoring their need for certifications based on their personal growth, with most choosing to begin their certification journey within the first year at a new company. Those with one year of experience or less at their organization are even more eager to use certifications as a means to improve their skills (69%) vs. those who have been at their companies for more than two years (62%) (see figure 37).

96% of respondents within our survey have at least one certification.

FIGURE 37

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



New employees

Those at organizations for **one year or less** are more eager to improve skills **(69%)** with certifications vs. those at organizations for **more than two years (62%).**

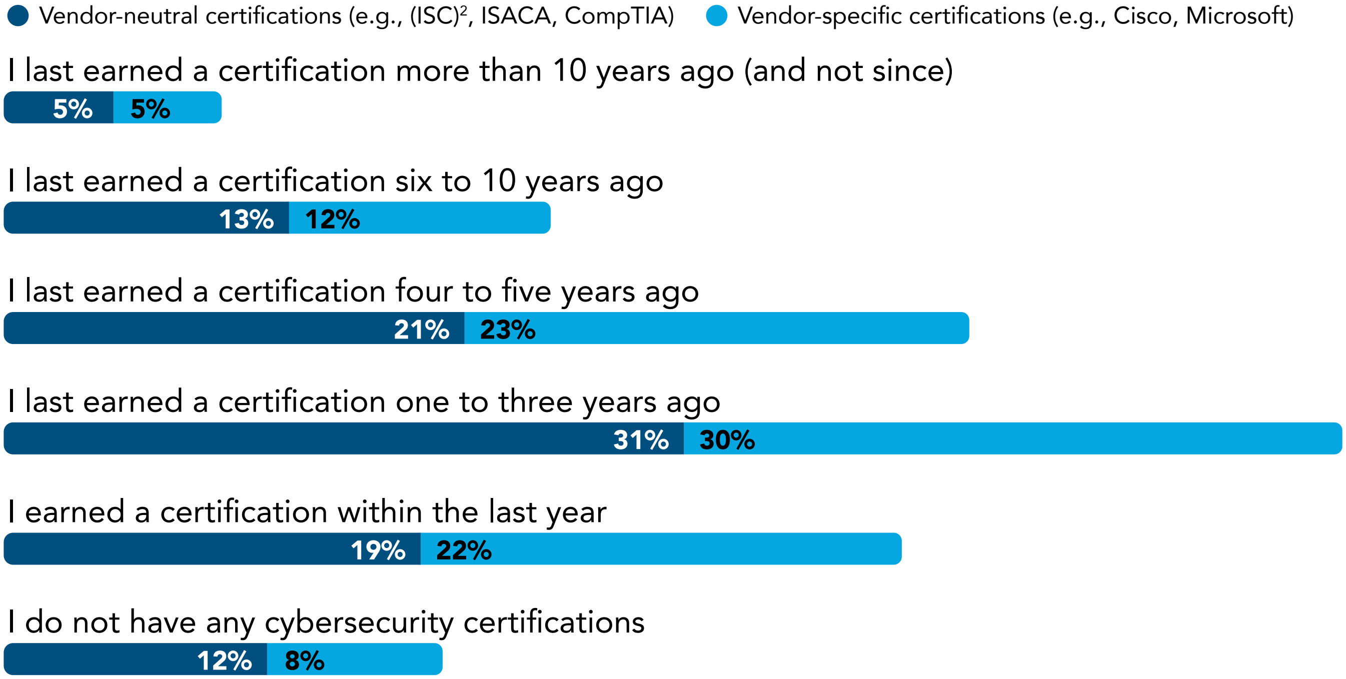
Base: 9,626 global cybersecurity professionals who plan to earn a certification in the future

- **Organizations are supporting employees to get certifications – but don't always require them to.** Companies are stepping up their support of cybersecurity professional development, with more than half offering reimbursements for third-party certification exams (51%). This creates an environment where certifications are encouraged but not required. 22% of respondents stated that, in the past, certifications were required for promotion. Only 14% say that this is driving a future need for certifications.

- **Both vendor-neutral and vendor-specific certifications are popular.** 89% of our respondents stated that they earned at least one vendor-neutral certification, e.g., (ISC)², ISACA or CompTIA. 92% have earned a vendor-specific certification, e.g., Microsoft, Amazon, CISCO. 50% of respondents have earned a vendor-neutral certification within the last three years vs. 52% who've earned one from a vendor in the same timeframe (see figure 38).

FIGURE 38

Do you have any vendor-neutral or vendor-specific cybersecurity certifications? If so, when was the last time you earned one?

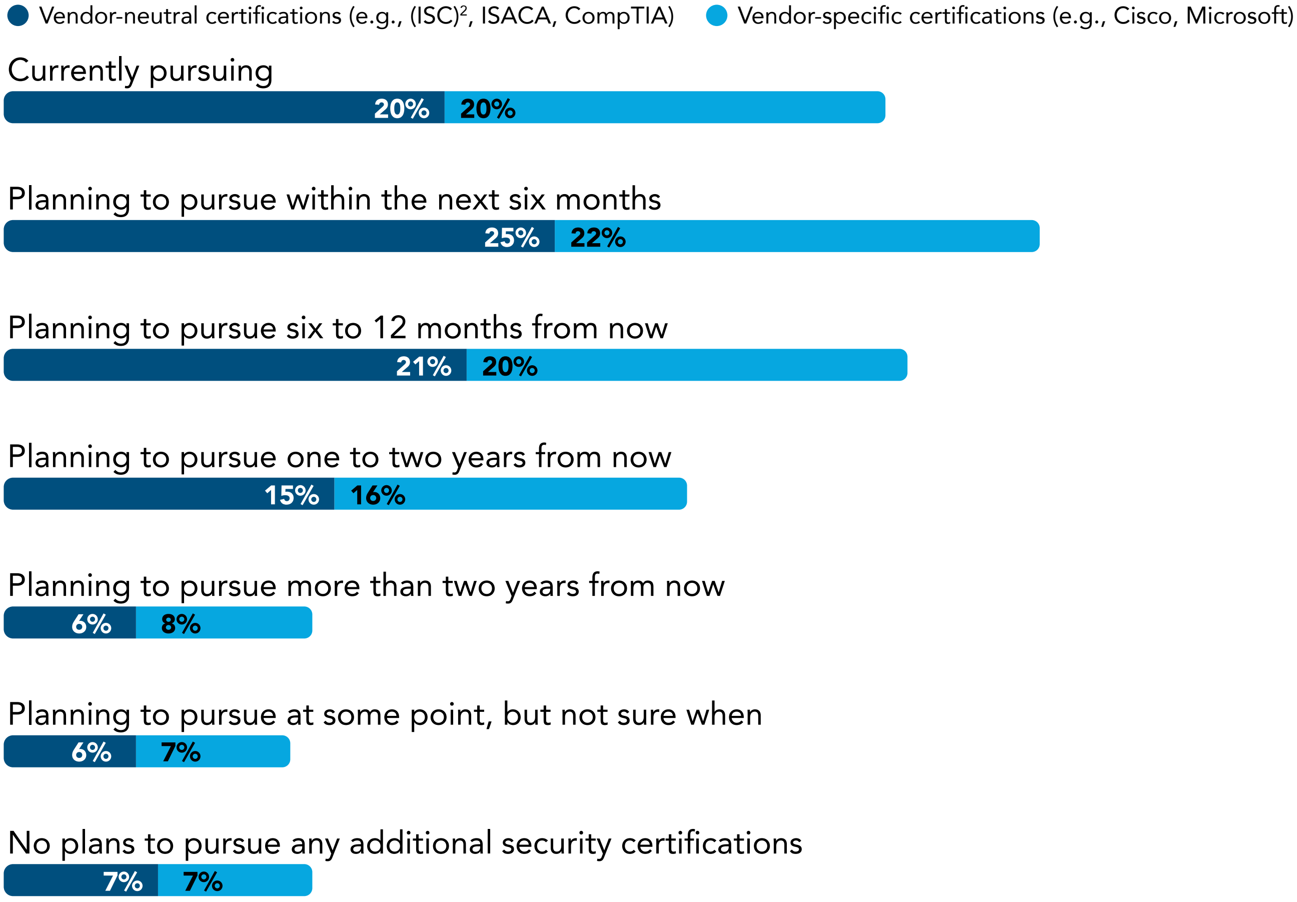


Base: 3,757 global cybersecurity professionals
Note: For questions related to certifications, the data shown represents data from a third-party survey panel. Part of this survey includes respondents from (ISC)²'s member base. They were excluded from these questions as to not skew the data.

66% are currently pursuing another vendor-specific certification or planning to earn one within the next year, and 62% are currently pursuing vendor-neutral certifications or planning to earn one within the next year (see figure 39).

FIGURE 39

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



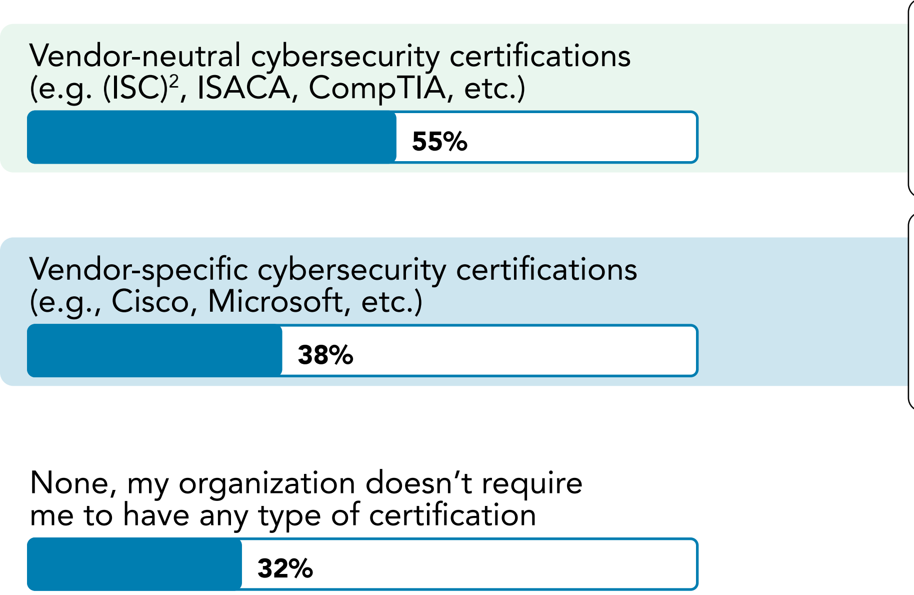
Base: 3,757 global cybersecurity professionals

Note: For questions related to certifications, the data shown represents data from a third-party survey panel. Part of this survey includes respondents from (ISC)^2's member base. They were excluded from these questions as to not skew the data.

Vendor-neutral certifications are more in demand from employers; 55% of which require their employees to have them. This is especially true for military personnel (82%). Comparatively, vendor-specific requirements have dropped within the last three years at an organizational level. In 2019, 55% of employers required them, vs. 38% in 2022 (see figure 40).

FIGURE 40

Which of the following types of cybersecurity certifications does your organization require you to have?



Vendor-neutral certifications are particularly ubiquitous among **military** (82%) personnel.

Requirements have dropped significantly in the past three years **(55% in 2019 vs. 38% in 2022).**

Base: 11,540 global cybersecurity professionals on cybersecurity teams

HOW MUCH DO CYBERSECURITY PROFESSIONALS MAKE?

We examined salaries by region and education level.

($) MEDIAN SALARY BY REGION

NORTH AMERICA	LATAM	EMEA	APAC
$134,800	$22,185	$93,535	$59,379

U.S.
$135,000

($) U.S. - EDUCATION-LEVEL

DOCTORATE/ POST-DOC	MASTER'S DEGREE	BACHELOR'S DEGREE	ASSOCIATE'S DEGREE/HIGH SCHOOL DIPLOMA
$150,000	$142,000	$130,000	$127,750

WHAT IT MEANS FOR ORGANIZATIONS

PATHWAYS AND CERTIFICATIONS

The workforce is changing from the bottom up, and we have observed that the next generation of cybersecurity employees is replacing traditional expectations with new pathways and skill sets garnered from a broad range of educational backgrounds, experiences and certifications.

Certifications define some of the most prominent and interesting trends within the industry. In some cases, cybersecurity professionals are using them and valuing them differently than their organizations are.

Our key takeaways for organizations that are defining their requirements and expectations for a new generation of employees are as follows:

- **Pathways: Recruit for a more diverse range of skills and perspectives.** Broadening your team's recruiting efforts beyond just those with IT experience is an opportunity to improve your risk mitigation strategy. Almost half of employees under 30 are coming into the cybersecurity profession with a background outside of IT, and those who do can add value and perspective to your organization's cybersecurity mission through different skills and experiences. Organizations that solely focus on recruiting for IT experience are narrowing their ability to evolve alongside the modern workforce.
- **Certifications: Use them as career builders, not barriers.** Cybersecurity professionals are not treating certifications as they used to: 64% of respondents seek new certifications for skills growth, rather than as a requirement for a job. In order to nurture new skills and passionate work within employees, don't use certifications as a barrier to entry. Do more to incentivize them. This trend has already begun, with more than half of organizations offering reimbursements for third-party certifications and others easing their requirements around vendor-specific certifications – this represents a decrease from 55% in 2021 to 38% in 2022. Almost half of employees under 30 are coming into the cybersecurity profession with a background outside of the IT industry. Embrace this trend by diversifying recruiting efforts.

Data Breaches, War and Modern Threats

Global cybersecurity professionals are reacting and adapting to more than just a fast-growing shift to remote work. The first half of 2022 was marked by both high-profile data breaches and the Russia-Ukraine war. Organizations big and small are measuring their own cybersecurity efficacy in the wake of corporate risk and military conflict. These heightened threats have increased corporate attention on organizations' cybersecurity teams, thus raising the bar for expectations and creating more work for employees.

Despite a volatile threat landscape and increased corporate and macroeconomic pressure, cybersecurity professionals are evolving and adapting to meet modern challenges head-on.

Here is what we learned about the impact of current events on the cybersecurity profession:

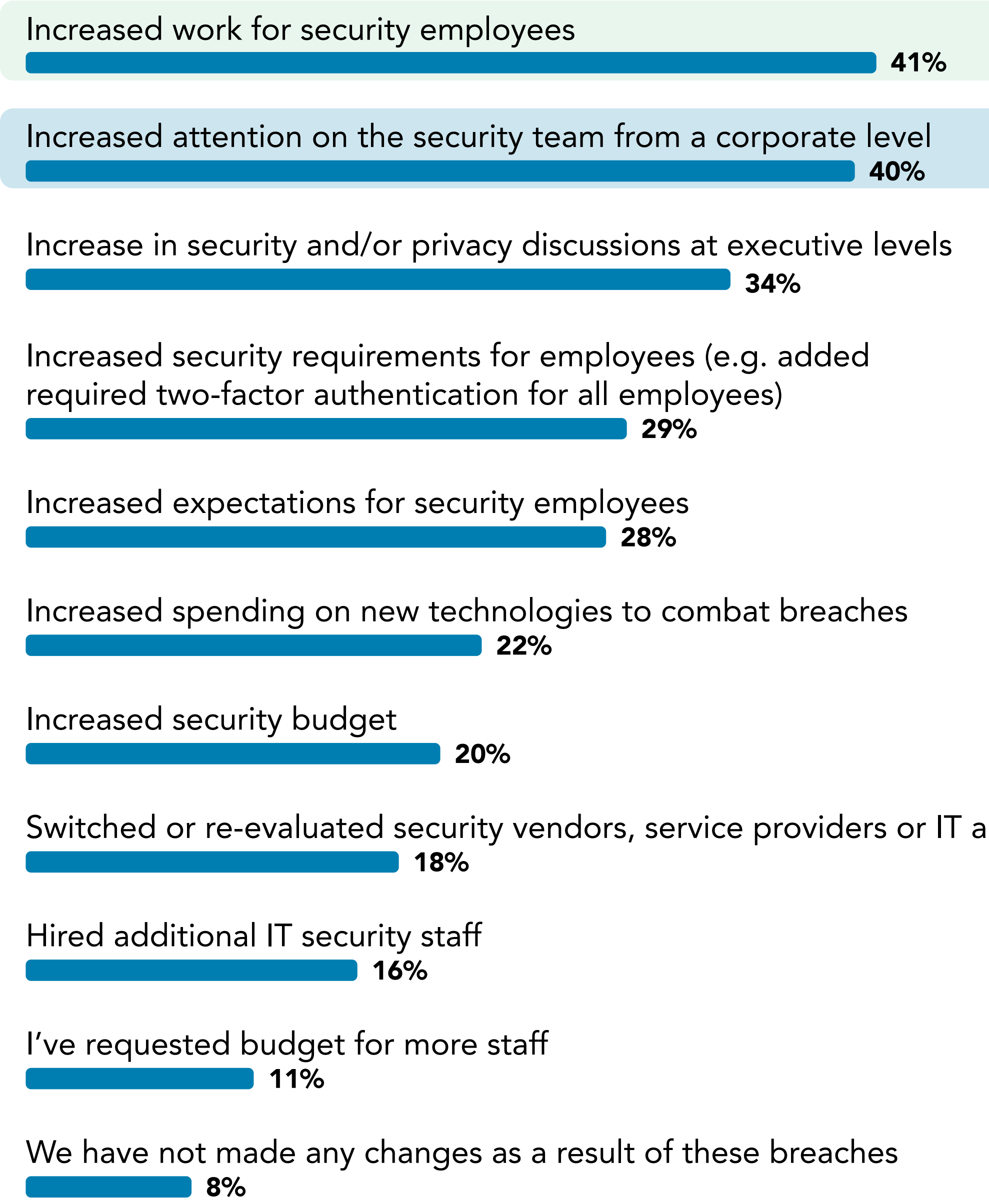
- **High-profile data breaches increase organizational focus on cybersecurity, but often at employees' expense.** In the wake of a highly publicized cybersecurity breach, the general public turns their attention to the cybersecurity profession. But how does it react to this spotlight? We found that the most common impact, which was felt by 41% of respondents, is an increase in work. This is amplified in certain industries, such as financial services (54%), aerospace (54%), government (53%) and military (51%).

  Although increased workloads and more attention from executive staff are common reactions to a data breach, there is also a lack of top-down support, which puts more pressure on employees. Only one in five respondents stated that their organization would increase their cybersecurity budget in response to a high-profile data breach. And an even smaller minority (16%) stated that their organizations would hire additional staff.

Similarly, executives pay more attention to their enterprise-wide cybersecurity vulnerabilities after a newsworthy data breach or attack takes place. 40% of our respondents state that they have experienced an increased interest in their cybersecurity team following a data breach – and this is even more significant within financial services (50%) and insurance (49%) industries (see figure 41).

FIGURE 41

How have recent high-profile security breaches and vulnerabilities (e.g., Okta, Log4J, SolarWinds) affected your security team?



High Impact Industries:
Financial services – 54%
Aerospace – 54%
Government – 53%
Military – 51%

High Impact Industries:
Financial services – 50%
Insurance – 49%

Base: 11,779 global cybersecurity professionals

Within our research, we learned that dissatisfaction within the workplace often stems from an organizational level, and this is a prime example of why that might be. Organizations need to support their employees by giving them the tools they need to defend themselves and their organizations. By doing so, the scope and scale of future data breaches may be mitigated by professionals who are not only more prepared, but more satisfied with where they work and who they work for.

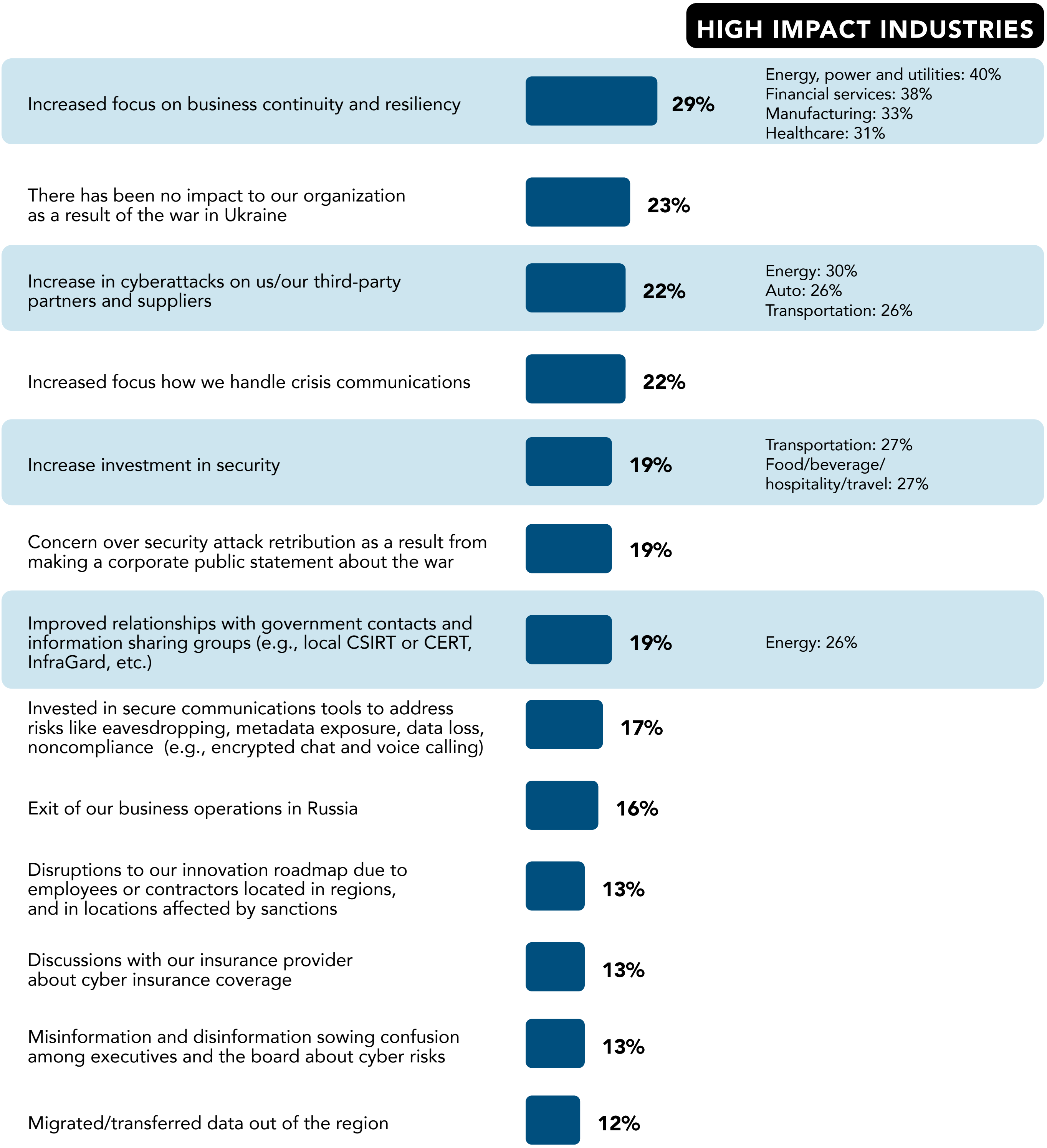
- **The Russia-Ukraine war is galvanizing action within specific industries.** Global organizations across all industries have been impacted in different ways by the Russia-Ukraine war. On average, the most significant impact across all organizations has been an increased focus on business continuity and resiliency (29%), followed by an increase in cyberattacks (22%), more focus on handling crisis communications (22%) and increased investment in cybersecurity (19%) (see figure 42). However, regional, industrial and employee size differences create a more detailed impact analysis.

  EMEA (31%) and North America (30%) have been more focused on business continuity and resiliency (31%) when compared with APAC (26%). Smaller organizations are not as concerned with business continuity and resiliency (selected by 18% of companies with less than 100 employees), as compared to larger organizations (22% response from companies with less than 100 employees).

  Travel-related organizations have been especially spurred into defensive action. 27% of respondents within the transportation and food/beverage/hospitality/travel industries are already increasing their cybersecurity investments as a result of the war. Some of this response is contextualized by the fact that more than 25% of transportation, automotive, energy, power and utilities organizations have experienced an increase in cyberattacks as a result of the war. The most significant industrial impact is an increased focus on business continuity and resiliency, which is felt within the energy, power and utilities (40%), financial services (38%), manufacturing (33%) and healthcare (31%) sectors.

FIGURE 42

What impact has your organization experienced as a result of the war in Ukraine?



Base: 11,779 global cybersecurity professionals

- **Despite the challenges of the modern cybersecurity landscape, most feel confident in their ability to mitigate risks.** At an industry level, our research is meant to get a pulse on those that are most prepared to defend themselves from future attacks. We found that cybersecurity professionals in the following industries are the most confident in their organizations' ability to do so: food/beverage/hospitality/travel (81%), security software/hardware development (75%), insurance (72%), construction (72%) and engineering (71%) sectors. Cybersecurity professionals in the five industries with the lowest confidence levels (e.g., transportation, education, healthcare, military/military contractors and government) were still more than 60% confident in their organizations' abilities to mitigate cybersecurity risks (see figure 43).

FIGURE 43

"Despite a challenging threat landscape, we are able to adequately mitigate risks."

(Percentages showing Agree/Strongly Agree responses)

TOP 5	
81%	Food/beverage/hospitality/travel
75%	Security software/hardware development
72%	Insurance
72%	Construction
71%	Engineering

BOTTOM 5	
65%	Transportation
64%	Education
63%	Healthcare
62%	Military/military contractor
61%	Government

Base: 115-1,220 global security professionals

WHAT IT MEANS FOR ORGANIZATIONS

DATA BREACHES, WAR AND MODERN THREATS

Each year, news of high-profile data breaches and geopolitical strife make their way to the executive desks at organizations across the world. These individuals raise their cybersecurity alarms in an attempt to mitigate the impact that something like this could have on their company and its assets. However, effective mitigation relies not only on employees carrying out the work but also on the support that those employees have. Our key takeaway is as follows:

- **Provide employees with top-down support to effectively mitigate risks.** As we have learned in our study, the most common impact felt by our respondents after a high-profile data breach has been an increase in work (41%). This burden falls directly on the shoulders of employees on the front lines of defense. This responsibility needs to be a top-down, bottom-up mission in which those on the front lines are armed with the support and tools they need to holistically defend their organizations. EX suffers when employees don't feel supported, so the way to retain staff and mount up for a potential cyberattack is to support the people who defend you.

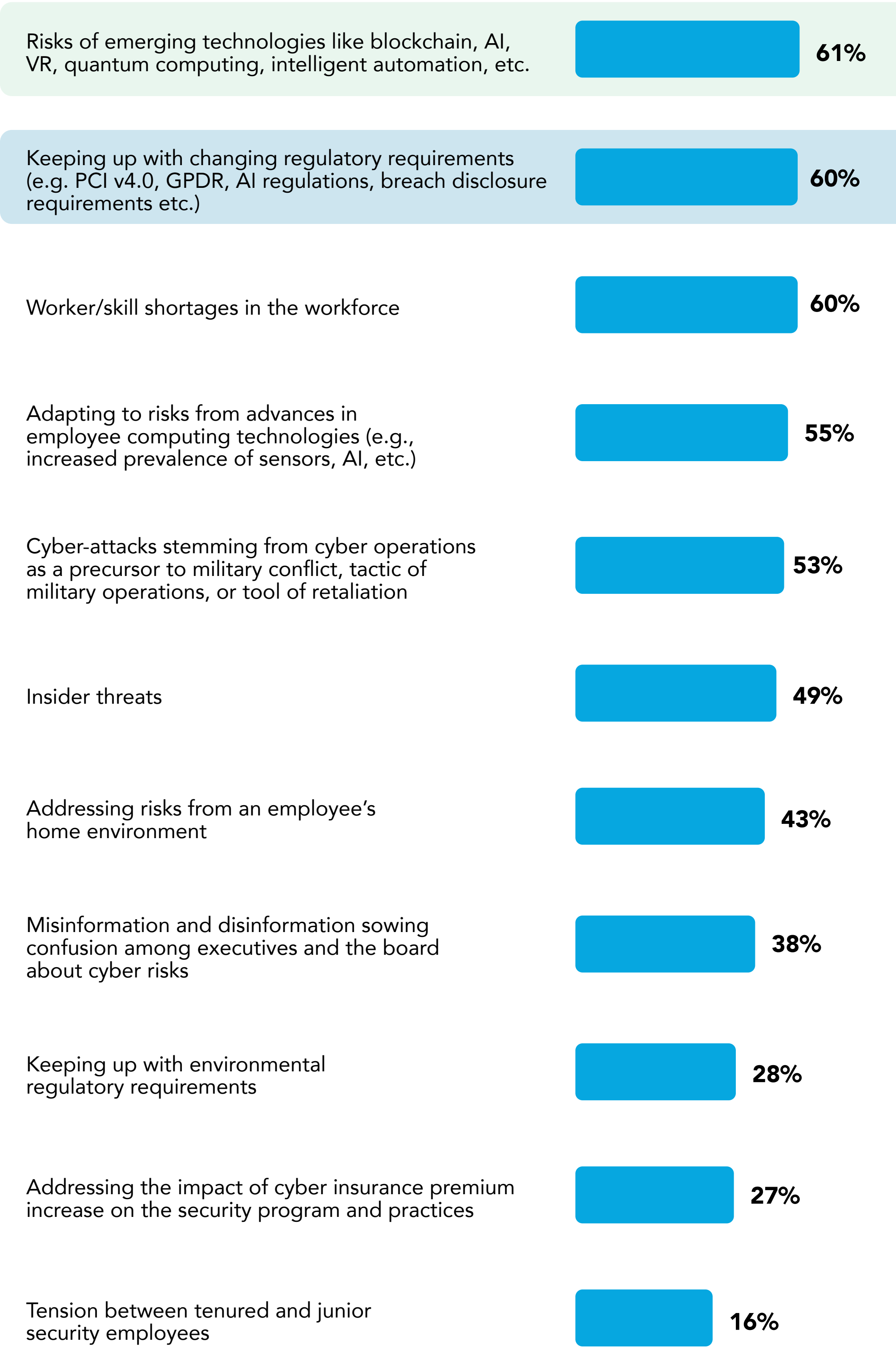
Future of Cybersecurity Work

While it is important to evaluate the landscape of the current cybersecurity profession, it is also critical to look to the future. Amidst the geopolitical conflict, macroeconomic turbulence and high-profile data breaches, cybersecurity has become an intensely important function for organizations worldwide. So, what waits on the horizon? We asked our respondents to identify the challenges, improvements and trends they will face going forward as well as their organizations' preparedness to handle new, anticipated risks. Here is what we learned:

- **Future challenges are rooted in emerging technology, the changing regulatory landscape and skills shortages.** Our research shows that over the next two years, 61% of cybersecurity professionals are primarily concerned by the potential risks of emerging technology (e.g., blockchain, AI, VR, quantum computing, etc.). This is closely followed by the 60% who are concerned about keeping up with regulatory requirements (e.g., PCI DSS v4, GDPR, AI regulations, etc.) and those who consider worker/skill shortages to be a continued risk (60%) (see figure 44).

FIGURE 44

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



APAC is most concerned about this, particularly in **China (68%) and South Korea (65%).**

North America (69%) is most concerned about this.

Base: 11,779 global cybersecurity professionals

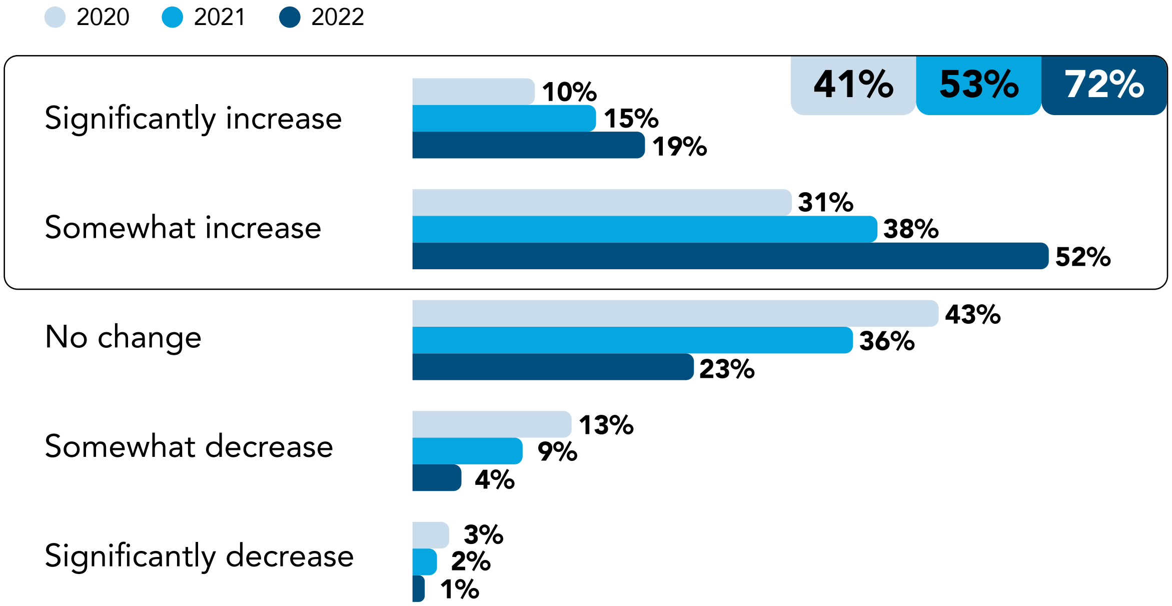
These risks vary across regions, and when we look closer at our research, we can see that the cybersecurity professionals in the APAC region (65%) – primarily China (68%) and South Korea (65%) – are much more concerned about the cybersecurity risks of emerging technology within the next two years, compared with LATAM (62%), North America (60%) or EMEA (59%).

Not all risks are concentrated in APAC. North American cybersecurity professionals are significantly more concerned about skill shortages than others, with 69% of respondents saying that this will be a future challenge. As we learned in our corporate culture research, the turnover rate in the US and Canada grew from 13% to 21% year-over-year, and this may explain some of the regional significance in skills shortage, especially since skills shortages are considered much less of a risk in EMEA (56%), APAC (50%) and LATAM (47%).

- **Despite risks and regional differences, cybersecurity professionals expect staff to grow at a much higher rate in the future.** Within the next 12 months, 72% of respondents expect staff to increase somewhat or significantly. This is the highest predicted growth rate over the last three years, compared to 53% in 2021, and 41% in 2020. It suggests an optimistic outlook on the future of the cybersecurity profession's growth, despite current and near-term risks. The question is, will the supply of new workers be able to keep up with the increase in demand? Regionally, LATAM (81%) and EMEA (76%) respondents are significantly more confident of an increase in staffing levels, whereas APAC (71%) and North America (68%) are still positive but a bit below the average (see figure 45).

FIGURE 45

How do you expect your organization's total staffing for cybersecurity to change 12 months from now compared to current levels?



Base: 11,525 global cybersecurity professionals on cybersecurity teams

- **Across industries, some have the skills and tools needed to mitigate long-term risks, and some don't.** We asked our respondents how much they agreed that their organization has the tools and people needed to respond to cybersecurity incidents over the next two to three years. The most confident responses we received were comprised of 66% of cybersecurity professionals working at cybersecurity software/hardware development companies. In addition, 65% of respondents working within construction, food/beverage/hospitality/travel and retail/wholesale agreed or strongly agreed that they have the tools and people they need to mitigate future risks. IT services (61%) was also within the top five most confident industries.

  Respondents within the public sector and government-related industries were least confident in their ability to mitigate long-term risks based on their current staff and tools; aerospace (50%), education (47%), healthcare (47%), military/military contractors (43%) and government (42%) were the lowest we observed (see figure 46).

FIGURE 46

"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."

(Percentages showing Agree/Strongly Agree responses)

TOP 5	
66%	Security software/ hardware development
65%	Construction
65%	Food/beverage/ hospitality/travel
65%	Retail/wholesale
61%	IT services

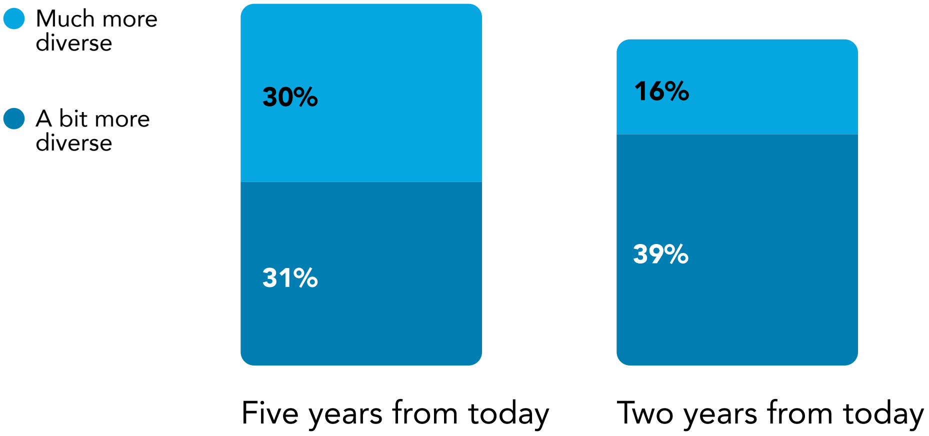
BOTTOM 5	
50%	Military/military contractor
47%	Healthcare
47%	Education
43%	Aerospace
42%	Government

Base: 115-1,220 global cybersecurity professionals

- **The future of cybersecurity is growing more diverse.** Our research has shown that pathways are opening for educated professionals with diverse backgrounds and cultures, but will this continue in the future? We asked respondents this very question and received their predictions about the next few years. We particularly wanted to know how their own team is likely to evolve. 55% believe that their team will become more diverse two years from now. Five years into the future, there is an even greater confidence in diversity, with 60% of respondents predicting more diversity (30% of which say it will be much more diverse) (see figure 47).

FIGURE 47

When thinking about how your cybersecurity team is likely to evolve, please tell us how more or less diverse you expect it to be in the next few years (e.g., increased representation across age groups, gender, race, sexual identity, disabilities, etc.).



Base: 8,092 global cybersecurity professionals who have worked at the same organization for two or more years

- **In a post-pandemic world, the normalcy of remote work continues to spread.** The pandemic has left a lasting impact on this profession, as it has with many others – changing workers' expectations and their satisfaction levels around their commutes and flexibility. This is putting pressure on organizations to now adapt and provide their employees with what makes them the most satisfied and productive, in order to prevent attrition. This has had a clear impact on the expectations of our respondents. When asked if they expected to be working remotely or on a flexible basis, the same amount of people who are working fully remote now or have the flexibility to do so (55%) expect to stay that way two years from now.

Conclusion

The need for more cybersecurity professionals is increasing. As the global landscape of geopolitical and economic risks evolves, so does a steadfast field of multi-cultural and multi-generational workers. We have heard from cybersecurity professionals with a wide range of perspectives across the world, and they are telling us that they are rewarded by their careers and adaptable to internal and external challenges in the workplace.

Our research suggests that the cybersecurity workforce is driven by a passion for what they do; and they have the best experience when they are able to chart their path and progression in the field. However, this experience is diluted when employees do not feel supported by the groups they work for. Individual employees need to be supported by their collective teams and organizations. Staff retention continues to be an issue, and although there is optimism about hiring/recruiting in the future, companies need to take more action to inspire loyalty and mitigate attrition. Showing employees that they are valued and listened to will improve their experience within the workplace (whether it's remote or on-site).

To improve, more organizations need to follow the example that others have set by supporting their employees' career growth through certification reimbursements, professional development offerings and mentoring programs. Improving the employee experience and giving professionals the tools they need to succeed is key to reducing the global gap in skilled cybersecurity staff.

Appendix A: Estimation Methodology

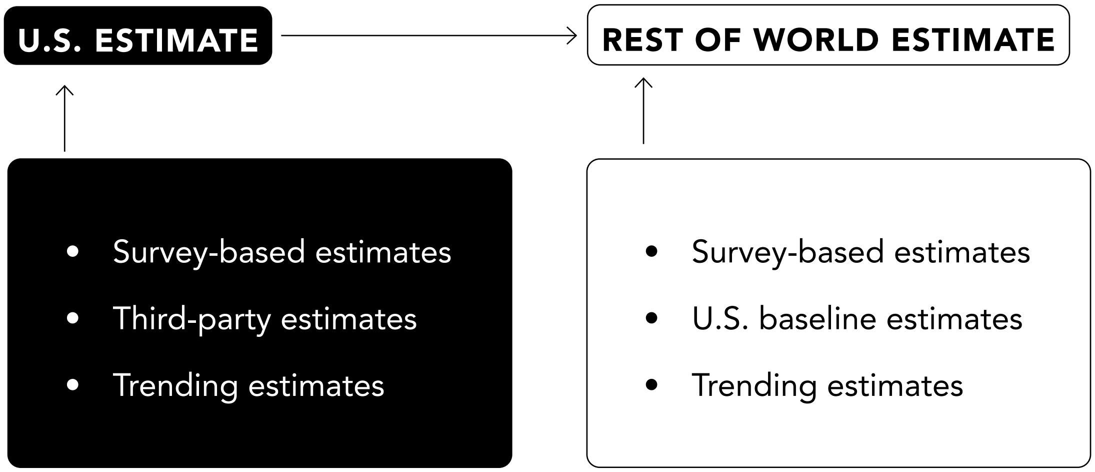
This year, our method compiles a variety of secondary data sources in combination with proprietary survey data to create a single, holistic estimate. This tactic of combining multiple different methodological approaches keeps any single number from disproportionately influencing the final estimate.

WORKFORCE ESTIMATE METHODOLOGY

The estimate of the global cybersecurity workforce begins with estimates of the U.S. workforce, as the U.S. provides a crucial combination of a robust sample and reliable secondary data sources. The U.S. 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 U.S. business entities in various size strata. These secondary sources include: the U.S. Bureau of Labor Statistics's Quarterly Census of Employment and Wages; the U.S. Census's Statistics of U.S. Businesses Survey; and the U.S. 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 U.S. 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 U.S. 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 U.S. baseline; most countries did not have reliable third-party estimates. The secondary data estimates for countries outside of the U.S. 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.



U.S. ESTIMATE

- Survey-based estimates
- Third-party estimates
- Trending estimates

REST OF WORLD ESTIMATE

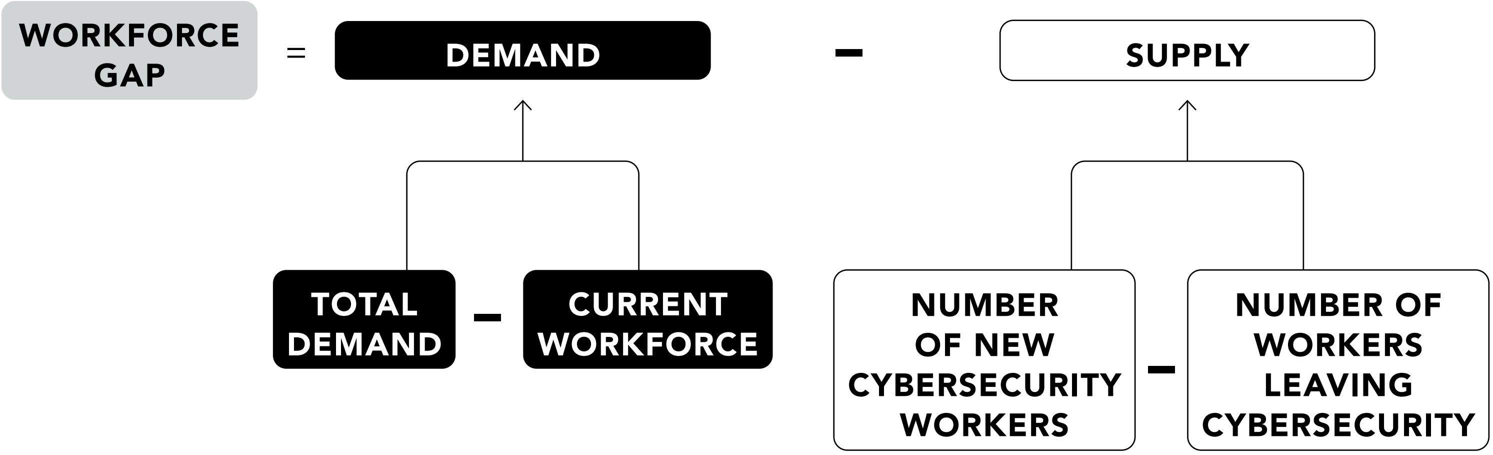
- Survey-based estimates
- U.S. baseline estimates
- Trending estimates

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 U.S. 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 that will enter the field over the next 12 months minus the number of workers that 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	**23%**
10,000-19,999	**6%**
5,000-9,999	**9%**
2,500-4,999	**9%**
1,000-2,499	**12%**
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%**

ROLE	
IT Manager	**9%**
IT Security Manager	**7%**
Security Engineer	**6%**
IT Director	**6%**
Security Consultant/Advisor	**5%**
Security Architect	**4%**
IT Specialist	**4%**
IT Security Director	**4%**
Security Analyst	**4%**
CISO	**4%**

INDUSTRY (TOP 10 SHOWN)	
IT Services	**25%**
Financial Services	**11%**
Military/Military Contractor	**9%**
Government	**8%**
Consulting	**6%**
Healthcare	**4%**
Telecommunications	**4%**
Manufacturing	**4%**
Security Software/Hardware Development	**4%**
Education	**3%**

RESPONDENT LEVEL	
C-level executive	**4%**
Executive management	**7%**
Director/Middle manager	**21%**
Manager	**22%**
Non-managerial mid or advanced level staff	**38%**
Entry/junior-level staff	**3%**
Independent contractor/consultant	**4%**

Base: 11,779 global cybersecurity professionals on cybersecurity teams

DEPARTMENT	
IT	**42%**
Security/privacy	**58%**

FULL TIME/PART TIME	
Employed/self-employed full time	**97%**
Employed/self-employed part time	**3%**

INTERNAL/EXTERNAL	
Internal security staff for my organization	**64%**
Security consultant or consultancy	**20%**
External security service provider (e.g., MSSP, external SOC, independent contractor etc.)	**10%**
Other	**5%**

TIME SPENT ON SECURITY	
100% of a typical week	**17%**
75% - 99%	**23%**
50% - 74%	**26%**
25% - 49%	**23%**
1% - 24%	**12%**

AREA OF FOCUS (NICE FRAMEWORK)	
Analyze	**11%**
Collect and operate	**6%**
Investigate	**4%**
Operate and maintain	**14%**
Oversee and govern	**30%**
Protect and defend	**12%**
Securely provision	**18%**

AGE	
74 or older	**0.1%**
65-73	**1.3%**
60-64	**3.9%**
55-59	**7.7%**
50-54	**11.7%**
45-49	**15.5%**
39-44	**21.3%**
35-38	**16.8%**
30-34	**14.7%**
23-29	**6.8%**
Under 23	**0.2%**

HIRING AUTHORITY	
I make final decisions about hiring	**29%**
I am part of a team that makes hiring decisions	**26%**
I interview candidates and influence decisions but do not make final decisions	**24%**
I do not have hiring authority or influence over decisions about hiring	**21%**

Base: 11,779 global cybersecurity professionals on cybersecurity teams

COUNTRY	
United States (US)	**38%**
United Kingdom (UK)	**7%**
Japan	**5%**
Canada	**5%**
China	**3%**
Germany	**3%**
Netherlands	**3%**
India	**3%**
Singapore	**3%**
Australia	**3%**
Brazil	**2%**
France	**2%**
Spain	**2%**
South Korea	**2%**
Republic of Ireland	**2%**
Mexico	**2%**
United Arab Emirates	**1%**
Saudi Arabia	**1%**
Nigeria	**1%**
Other	**9%**

Base: 11,779 global cybersecurity professionals on cybersecurity teams

STATE (TOP 20 SHOWN)	
Virginia	**11%**
California	**9%**
Texas	**7%**
Maryland	**6%**
Florida	**4%**
Colorado	**4%**
New York	**4%**
Pennsylvania	**3%**
Georgia	**3%**
Washington	**3%**
Illinois	**3%**
North Carolina	**3%**
Ohio	**3%**
Massachusetts	**2%**
New Jersey	**2%**
Arizona	**2%**
Alabama	**2%**
Minnesota	**2%**
Michigan	**2%**
Utah	**1%**

Base: 4,507 global U.S. cybersecurity professionals on cybersecurity teams

GENDER OF RESPONDENTS	
Female	**17%**
Male	**78%**
Intersex	**0.2%**
Transgender	**0.3%**
Non-binary	**0.3%**
Prefer to self-describe	**0.2%**
Prefer not to say	**4%**

Base: 11,779 global cybersecurity professionals on cybersecurity teams

Note: The demographic distributions of gender, race and ethnicity should be considered a representation of the survey sample and not necessarily reflective of the cybersecurity industry as a whole.

ABOUT (ISC)2

ISC)² is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)² offers a portfolio of credentials that are part of a holistic, pragmatic approach to security. Our association of candidates, associates and members, more than 235,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is supported by our commitment to educate and reach the general public through our charitable foundation – The Center for Cyber Safety and Education™. For more information on (ISC)², visit www.isc2.org, follow us on Twitter or connect with us on Facebook and LinkedIn.

ABOUT THE (ISC)² CYBERSECURITY WORKFORCE STUDY

(ISC)² conducts in-depth research into the challenges and opportunities facing the cybersecurity profession. The (ISC)² 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 2022 (ISC)² Cybersecurity Workforce Study is based on online survey data collected in collaboration with Forrester Research, Inc. in May and June 2022 from 11,779 individuals responsible for cybersecurity at workplaces throughout North America, Latin America (LATAM), the Asia-Pacific region (APAC), and Europe, Africa & The Middle East (EMEA). Respondents in non-English speaking countries completed a locally translated version of the survey. The sample size within each country was controlled to ensure a mix of company sizes and industries.

Learn more at www.isc2.org/research.