(ISC)²

Cybersecurity Professionals Stand Up to a Pandemic

(ISC)² CYBERSECURITY WORKFORCE STUDY, 2020

Table of Contents

Introduction

At organizations large and small, cybersecurity professionals have been thrown into an unprecedented storm this year, facing some of the toughest challenges of their careers. Despite an ongoing shortage of qualified cybersecurity personnel across public and private sectors, these professionals have been largely successful in overcoming new challenges and protecting their organizations.

This report explores the results of the 2020 (ISC)² Cybersecurity Workforce Study. Our survey collected data from 3,790 security professionals at all levels, drawn from small, medium and large organizations throughout North America, Europe, Latin America (LATAM) and the Asia-Pacific region (APAC).

This year the survey was fielded in late April 2020 through mid-June. The findings are unique in that they capture the mood and environment of the cybersecurity workforce in the midst of the COVID-19 pandemic. Our study reveals the significant impact COVID-19 has had on cybersecurity professionals and the challenges many of them had to overcome.

Beyond how cybersecurity professionals have fared during COVID-19, this year's study also provides an update to two very critical components of defining the industry's skills shortage—the Cybersecurity Workforce Gap and Cybersecurity Workforce Estimate. Each metric has a critical role to play in informing best practices and policies to encourage growth of the workforce and define success metrics. This is the second consecutive year we have produced a Cybersecurity Workforce Estimate, and our data suggests that the global cybersecurity workforce needs to grow 89% to effectively defend organizations' critical assets.

This report also examines the makeup of the workforce, with an eye to the challenges they face, skills they need to develop, job satisfaction, salary benchmarks, team composition, views on the value of certifications for staff and leadership, hiring trends and future organizational needs.

We conclude with actionable advice and key takeaways for cybersecurity professionals at all levels—staff, managers and senior leaders—who are responsible for securing critical assets around the world.

Cybersecurity Under Pressure

The COVID-19 pandemic has forced rapid changes in the world of cybersecurity, as it has in all facets of operations. While remote work is not new for some job roles, especially in technical fields, the workplace-wide shift to remote work has been sudden and wide-ranging, leaving security professionals with little time to respond. Similarly, while cloud services have been making inroads for well over a decade, the cloud has quickly moved from luxury cost saver to absolutely critical in today's economic environment.

Adding to the pressure, security professionals have had to address the transition to remote work within extremely short timelines. Some companies made the leap to remote work literally overnight, even while security professionals were unable to work from the office themselves. How smoothly this transition has been handled around the globe is a tribute to the skill and resilience of cybersecurity professionals at every level.

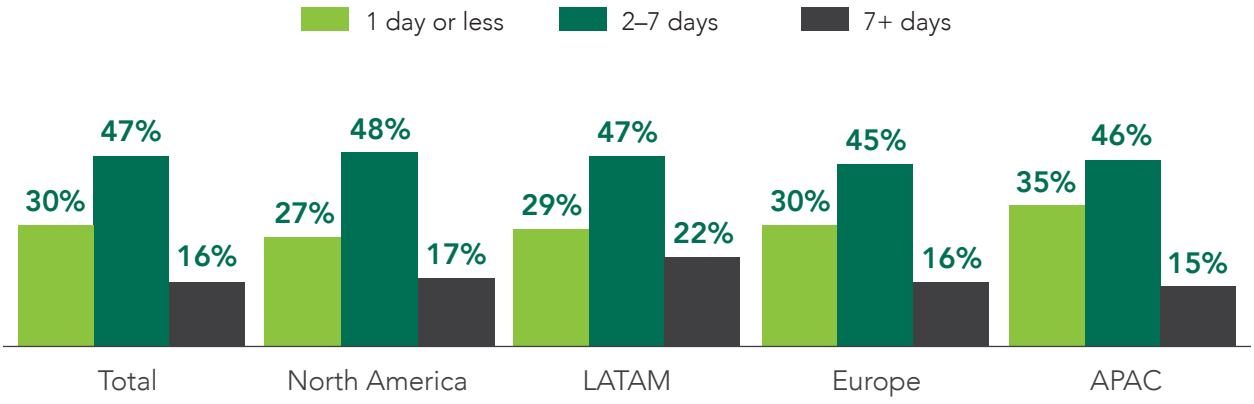
In many cases, they had only days (and sometimes only one) to help their organizations complete a massive shift to remote work. That meant getting user populations online rapidly, in many cases with vastly different network connectivity capabilities, devices and technical knowledge levels.

Worldwide, 30% of respondents reported that their organizations made the move to a remote workforce in a single day, while 47% were given several days to a week. Just 16% said that they had more than a week to make this shift.

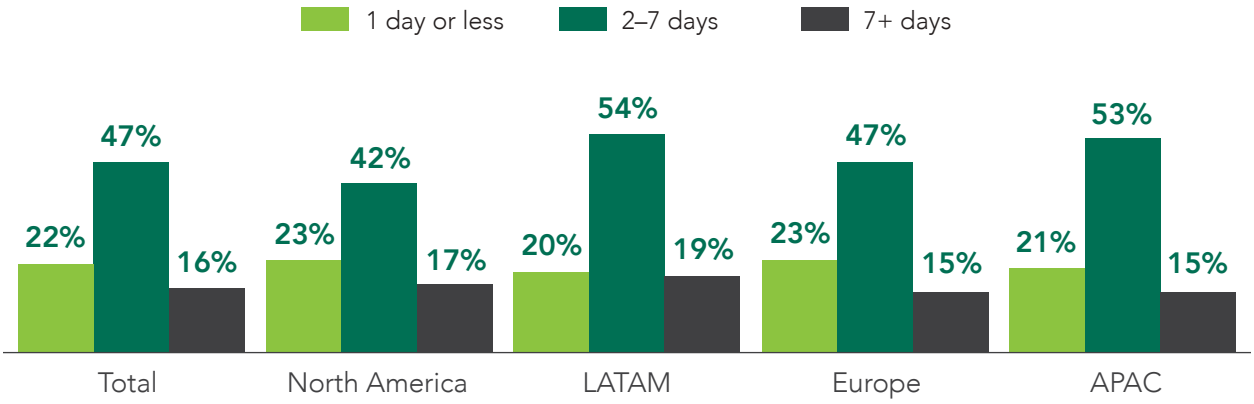
The physical logistics of moving to online work are accompanied by the parallel need to secure the newly remote workforce. Cybersecurity professionals reported facing largely similar timelines as they did for the move to remote: 22% had less than one day to ensure that remote systems were secured, while again 47% were allowed several days to a week, and only 16% had more than a week.

Notification Given to Move Workforce Remote

Cybersecurity professionals faced tight deadlines in transitioning employees to remote work and securing newly transformed IT environments.



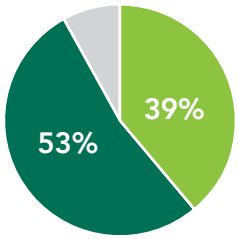
Length of Time to Secure Remote Workforce



Even in the face of rapidly changing environments, most cybersecurity professionals felt their organizations were well prepared for this shift. Despite the inevitable roadblocks they encountered, cybersecurity professionals said their organizations were able to respond effectively to COVID-19, with 63% rating their immediate response, and 64% rating their overall response as Excellent or Very Good; 92% of respondents reported their organizations were at least somewhat prepared for the transition, with 53% indicating they were very well prepared.

Organizational Preparedness for Remote Work Transition

Most cybersecurity professionals surveyed felt their organizations were prepared for the transition to remote work.



92%

are very or somewhat prepared

Somewhat prepared

Very prepared

"A well-developed and structured communications strategy helped with keeping all personnel well informed of what was going on, with setting the appropriate expectations, and with implementing any necessary changes."

– Study participant

Another bright spot for cybersecurity personnel is their belief that in the current crisis, their ability to function as part of effective teams is undiminished. 25% of respondents worldwide report that remote work has actually improved rather than diminished their team communications. Overall, only 12% of cybersecurity professionals reported worse communications because of remote work, and this percentage varied only slightly (from 8–15%) across all regions surveyed.

Remote Work Impact on Team Communication

Across regions, cybersecurity professionals overwhelmingly reported that team communications have either been unaffected or have improved as a result of remote work.

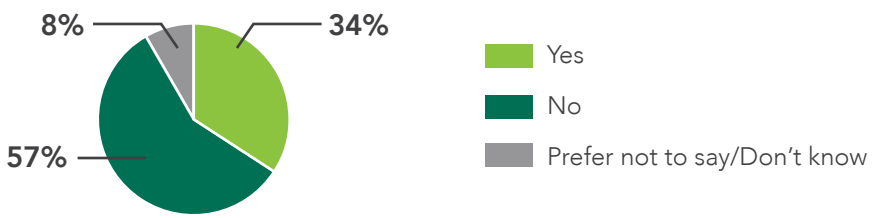
While management and senior leadership find remote work improves communications, general staff have seen no impact on communications.

> **"Our transition has been mostly seamless. The communications bit has been a learning curve to an extent, but we learned which tools worked and which didn't."**
>
> ***– Study participant***

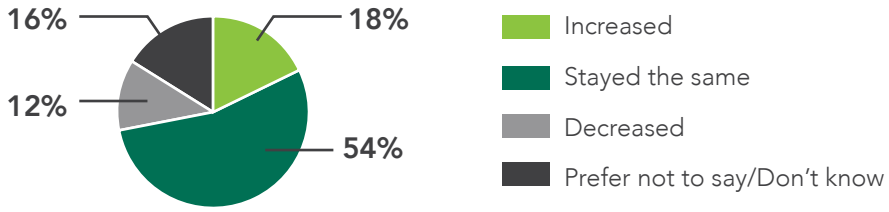
Perhaps most surprising, and a testament to the determination of the current cybersecurity workforce, is the percentage of respondents reporting that their organizations have not been compromised by having a remote security team.

Despite possibly greater vulnerability, most cybersecurity professionals report stable or even reduced numbers of security incidents. Only 18% of respondents worldwide reported a rise in security incidents in the wake of COVID-19, and 12% actually reported a decrease in incidents. This is impressive given that 35% of respondents worldwide, including 34% in North America, believed (at the time of the survey) that their organizations were actually more exposed to security threats, and 34% reported compromised readiness.

Compromised Security Readiness Due to Remote Security Team



Security Incidents After Transitioning to Remote



Senior leadership's understanding of the importance of security in remote work environments for their organizations may have contributed to the success in keeping security levels high: 67% of respondents worldwide report that organizational leadership is cognizant of its vital role.

Does Leadership Understand the Security Implications of Remote Work?

Security professionals say that organizational leadership understands the importance of security.

67%

of leadership understand the importance of security in remote work environments

Lack of leadership awareness has a real impact on teams. Morale was lowest for cybersecurity professionals who reported their leadership was not aware of remote work security implications.

Those at a manager level or higher are more likely to feel their organization's security readinesss has been compromised due to remote work than their cybersecurity staff.

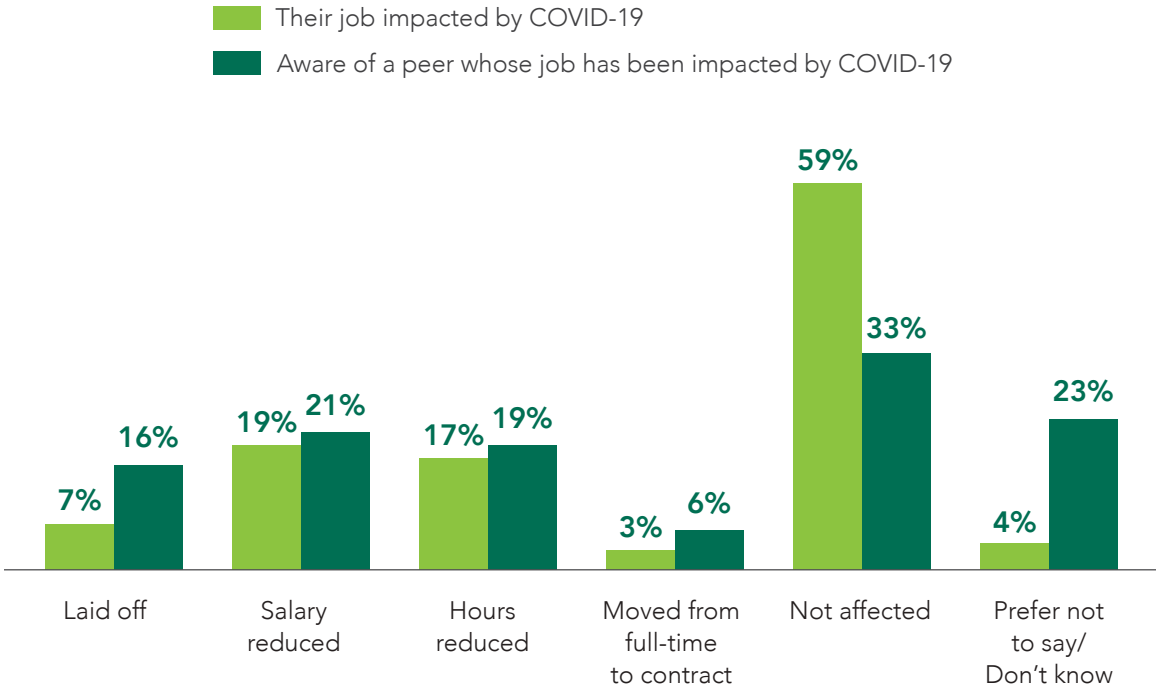
Those who took the survey in mid-May or earlier are more likely to feel their organization's security readiness was compromised, compared to those who took the survey in mid-May and later.

Despite this generally positive view of their ability to handle the crisis, and widespread support from management, cybersecurity professionals nonetheless faced and continue to face substantial difficulties. One understandable source of stress is the knowledge that business cutbacks and operational changes have affected many positions with layoffs, furloughs or salary cuts. While more than half of respondents say their own jobs have not been affected, many report awareness of other cybersecurity professionals who have been affected by these measures.

Additionally, 17% of respondents report that their hours have been reduced as a result of the pandemic, and 19% report a reduction in salary.

COVID-19's Impact on Cybersecurity Jobs

The majority of cybersecurity professionals report that their own job has not been affected, but some report impacts to hours, salary, or full-time status.

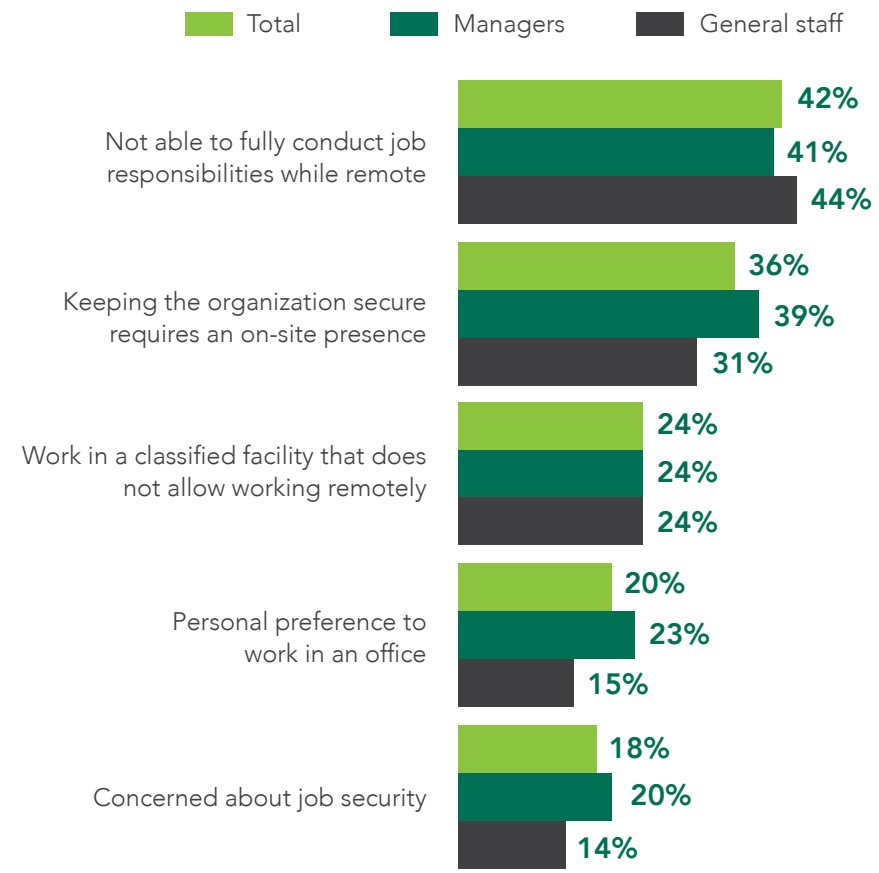


Emerging workplace habits and practices may raise the ability to go all-remote, but many cybersecurity professionals report that they still must do some of their work from a conventional workplace, or that they simply prefer to work in an office. For some cybersecurity professionals, necessary tasks include dealing with on-premises infrastructure, physically setting up other employees' machines, or complying with stringent data security rules for sensitive or secure government work.

Those at the manager level or above reported at significantly higher levels keeping their organizations secure required an on-site presence (39% vs. 31% of general staff). 20% of managers and above—compared to just 14% of general staffers—said that they were reporting to the office because they were concerned about their job security.

Reasons for Going into the Office

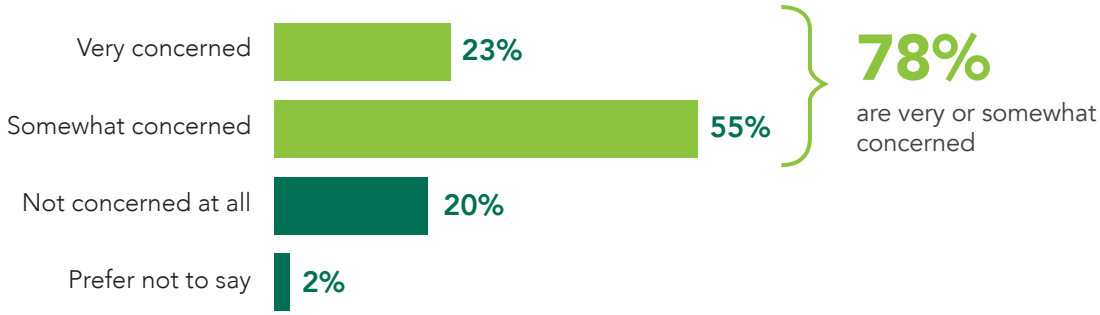
Despite global efforts to transition workplaces to remote work, many cybersecurity professionals still have to perform on-premises work. Here's why:



While the need still exists for in-office presence for some tasks, 78% of cybersecurity professionals worldwide still going into the office are somewhat worried, or very worried, about their health and safety.

Level of Concern About Own Safety

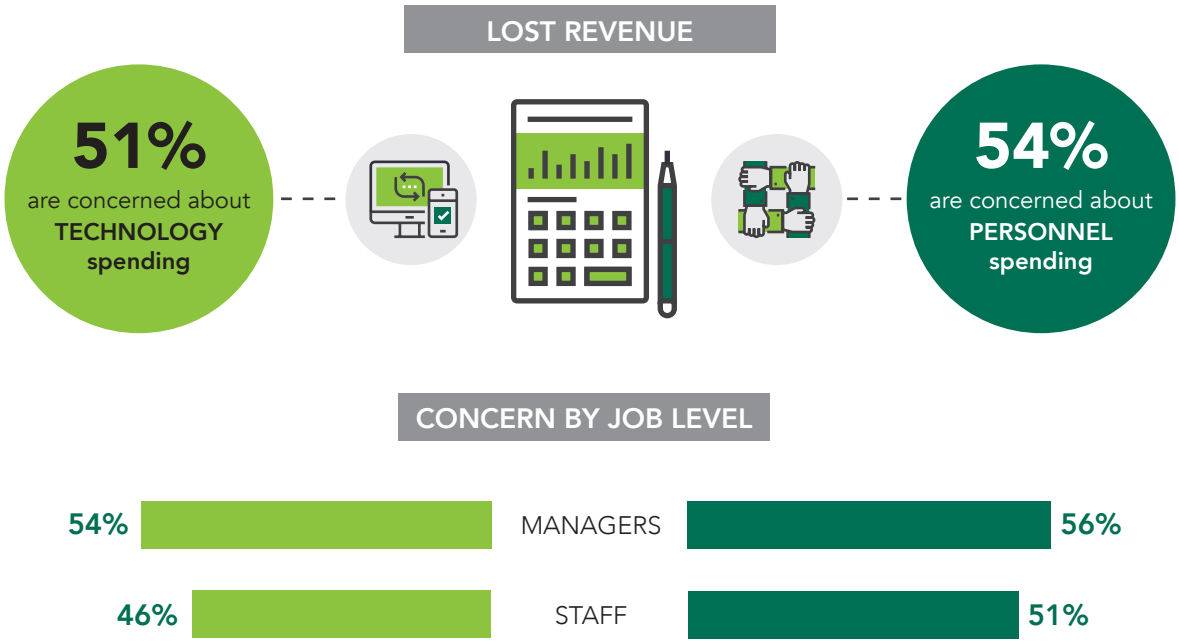
Worldwide, a majority of cybersecurity professionals that need to work from an office are worried about their own safety.



Cybersecurity professionals are working hard to do more with less under unprecedented circumstances. Respondents report staff shortages at more than half of their organizations, which means they have less time to deal with conventional security needs. Further compounding their challenges, more than half of respondents are expecting a negative impact on their organizations' budgets for technology and staffing this year, because of COVID-19-related revenue losses, with those in managerial or executive roles far more likely to expect tighter budgets. For personnel spending, 56% of managers and above expressed concerns, compared to 51% of general staff. The spread was even wider when it comes to technology expenditure: Only 46% of general staff expressed a concern that COVID-19 would cut into this part of the budget, compared to 54% of managers and above.

Security Spending Concerns

Cybersecurity practitioners are concerned security budgets will be impacted by revenue losses due to COVID-19.



> **"Cybersecurity has always been a value-added item in the budget when there was extra money. We were doing good to hold the line within my org until COVID-19 came along."**
>
> ***– Study participant***

The Cybersecurity Workforce Estimate and the Workforce Gap

The (ISC)² Cybersecurity Workforce Study is the result of an annual global survey of individuals responsible for cybersecurity at workplaces around the world, from small businesses to large enterprises, government agencies to educational institutions. The result is a set of tools to help everyone interested in solving the skills gap make smarter decisions, from hiring managers to policy makers.

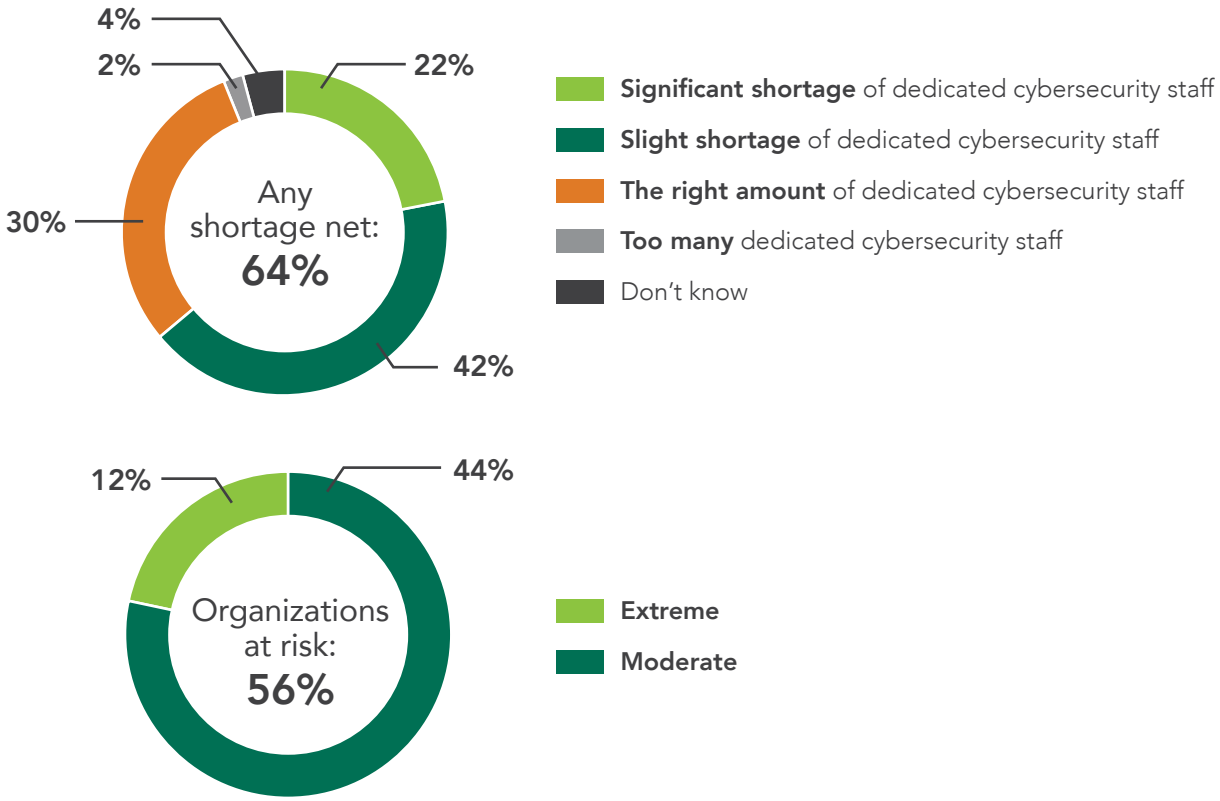
One key objective of the study each year is to estimate the size of the global cybersecurity workforce. Another, just as vital, is to better understand the industry's skills gap and uncover solutions for addressing the global talent shortage. This includes ensuring career-long professional development for those already in the field, identifying pathways into the workforce for new entrants, and helping employers identify existing and future sources of fresh talent.

This year, despite the economic challenges presented by COVID-19, for the first time ever we saw the Cybersecurity Workforce Gap decrease—from 4 million to 3.1 million.

It's worth noting that while actual security incidents have stayed at baseline levels, and despite the narrowed workforce gap, more than half of respondents (56%) say that cybersecurity staff shortages are putting their organizations at risk.

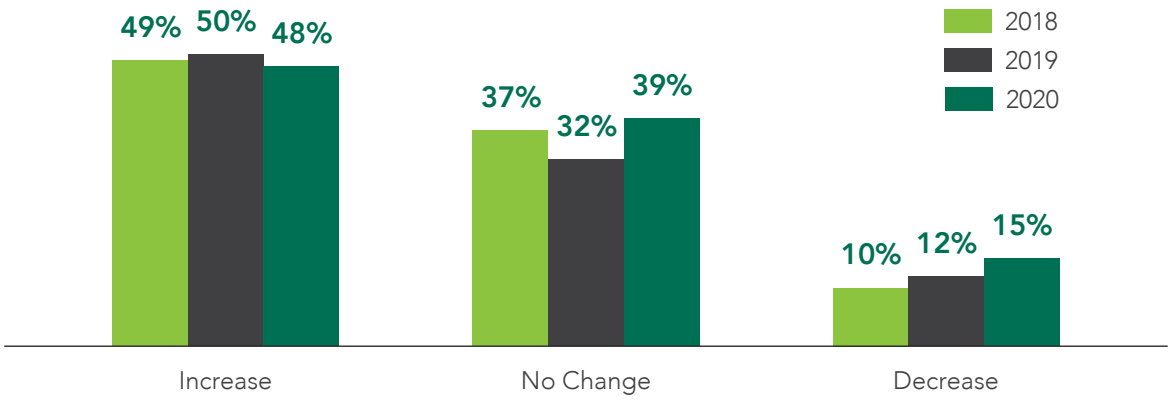
Cybersecurity Staffing Levels and Security Risks

Cybersecurity professionals report staff shortages at their own organizations, and security risks that spring directly from those shortages.



Expected Change in Cybersecurity Staffing Levels

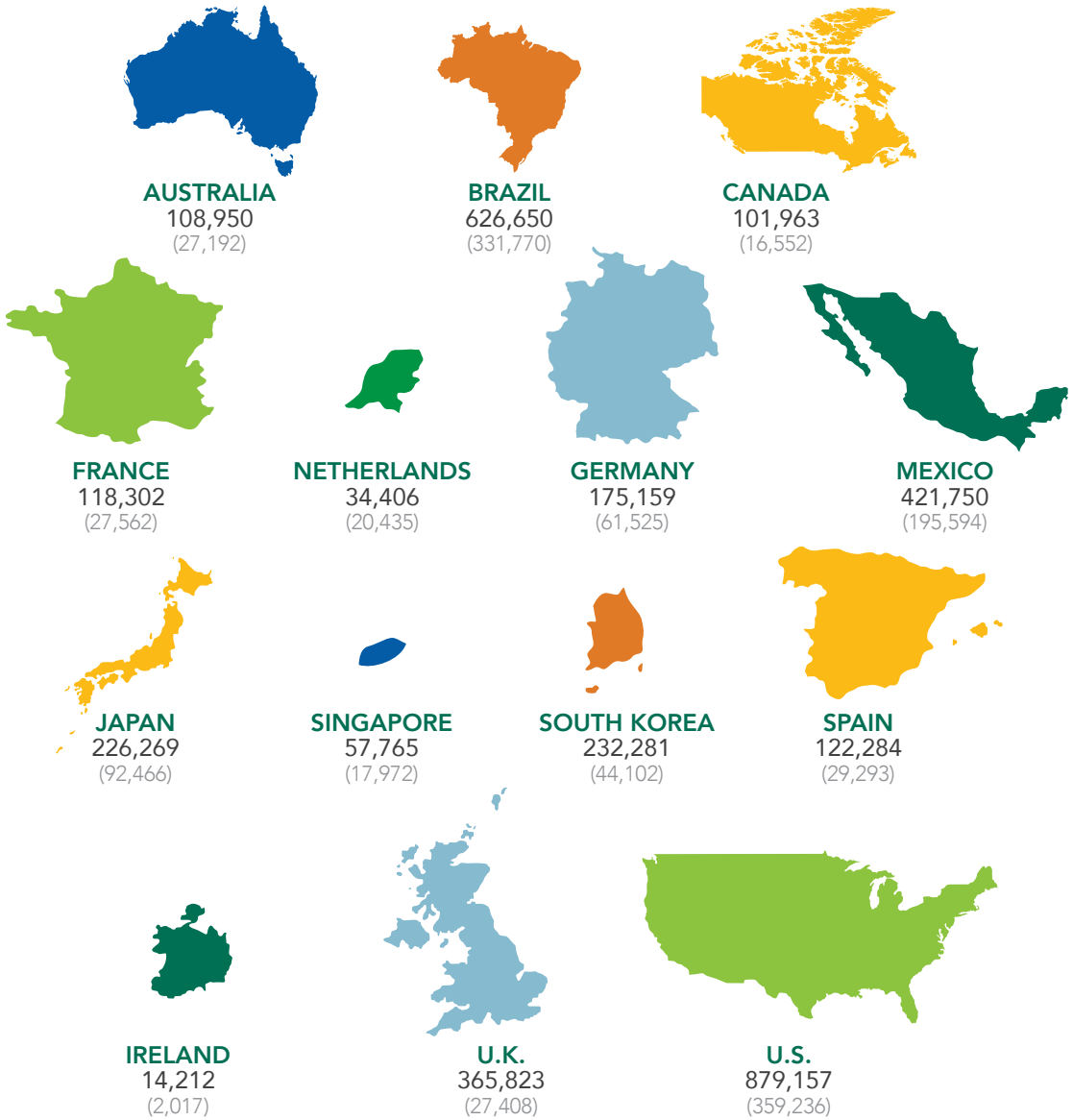
Despite COVID-19 and economic pressures, organizations' plans to increase cybersecurity staffing over the next 12 months remain consistent with previous years.



The size of the global workforce and of the corresponding workforce gap varies by region. While the largest single population of cybersecurity professionals is in the U.S., along with the largest cybersecurity gap, there are substantial cybersecurity talent pools all over the world, as well as ongoing cybersecurity personnel shortages.

Global Cybersecurity Workforce and Gap Estimates

The current cybersecurity workforce estimate is shown for each of the countries below, with the size of the workforce gap indicated in parentheses.

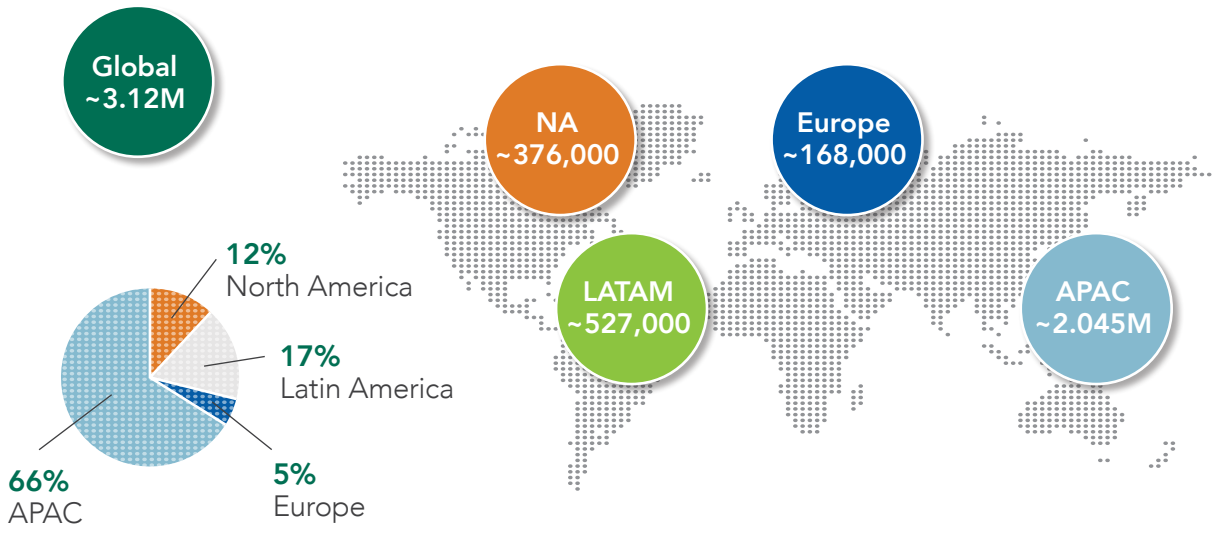


The cybersecurity workforce gap, simply put, is the difference between the number of skilled professionals that organizations need to protect their critical assets and the actual capacity available to take on this work. It is not an estimate of open positions available to applicants.

Our 2020 survey revealed that the gap between desired positions and those employed in cybersecurity has declined somewhat compared to previous years. Worldwide, the cybersecurity gap narrowed from 4 million worldwide in 2019 to 3.1 million. The gap in the U.S. shrank from 498,000 to 359,000, with a rest-of-world gap of 2.7 million.

The Cybersecurity Workforce Gap by Region

The global gap in the cybersecurity workforce varies by region, dominated by a gap of more than 2 million in the Asia-Pacific region.



WHY DID THE GAP SHRINK?

The smaller gap we see in 2020, despite business contractions and uncertainty, does not indicate a vastly greater number of security applicants. Instead, this is likely a combination of ongoing entry to the field coupled with reduced demand because of diminishing business requirements during the pandemic.

Factors That Have Contributed to This Change:

- The required workforce and hence the gap estimate depends directly on how businesses report investment in hiring cybersecurity professionals, and in 2020 investment projections are softer.
- Driving this trend is reduced average headcount demand in most company segments (excluding the largest employers). While U.S. demand is the biggest driver for the decrease, the worldwide trend is clear—no single country is showing year-on-year growth in demand, with stated demand globally down 5% from 2019.
- There is a sharp downshift in the estimated number of U.S. businesses that are investing in cybersecurity professionals, especially small and medium businesses. While slightly more large enterprises are investing in cybersecurity professionals compared to 2019, their actual 2020 hiring investment levels are lower.
- Supply is up year-over-year, which is likely driven by a strong base of industry migration. It also appears that a higher share of organizations are increasing supply by investing in their current base of professionals.

How the Survey Was Designed

The 2020 (ISC)² Cybersecurity Workforce Study is based on online survey data collected in April, May and June 2020 from 3,790 individuals responsible for cybersecurity at workplaces throughout North America, Europe, Latin America (LATAM) and the Asia-Pacific region (APAC). 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.

To fully understand cybersecurity needs and behaviors in the business sector, the (ISC)² survey included a global mix of certified professionals in official cybersecurity functions as well as IT/ICT professionals who spend at least 25% of a typical work week handling responsibilities specifically related to cybersecurity. These responsibilities could involve data security, security risk management/assessment, security compliance or threat detection/remediation, as well as network security architecture and monitoring, supporting or troubleshooting cybersecurity systems. Because professionals from every level of cybersecurity and IT/ICT were involved in the study, it presents a comprehensive picture of the practices, expectations and perceptions of managers and ground-level staff alike.

We heard from 553 more cybersecurity professionals than in 2019, continuing our goal of increasing the sample size and increasing the validity of the results. The margin of error for the global descriptive statistics in this research is plus or minus 1.6% at a 95% confidence level.

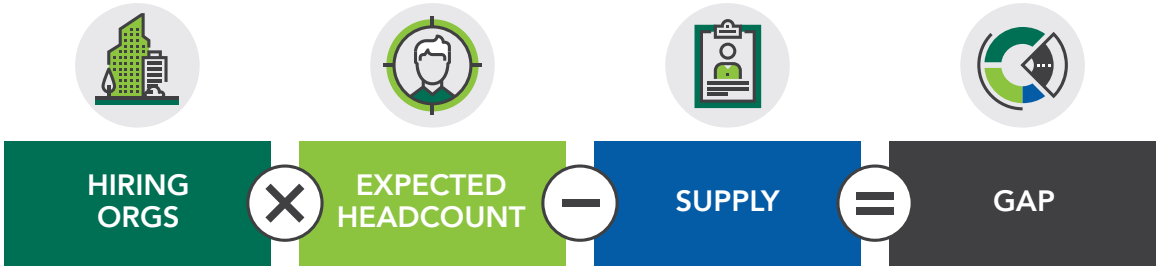
OUR ESTIMATION METHODOLOGY

Calculating the cybersecurity workforce gap requires more than simply subtracting a readily calculated supply from an easily predicted demand. The gap is never static, which is why we consider several critical factors, including the percentage of organizations with open positions and an estimation of anticipated staffing needs.

The calculation of supply includes estimates for new entrants to the workforce (from academic and non-academic backgrounds) as well as estimates of professionals currently in other fields who are pivoting to cybersecurity specialties. We've adopted this dynamic, holistic measurement approach to obtain a more realistic representation of the challenges and opportunities facing both companies and cybersecurity professionals worldwide.

Gap Calculation

Calculating the global workforce gap requires consideration of expected demand as well as estimated personnel counts.



The (ISC)² Cybersecurity Workforce Study provides a robust cybersecurity headcount across company sizes, but only among actual survey respondents. To extrapolate the cybersecurity headcount volume by country requires data from credible secondary sources (such as a national census) for the total count of operational businesses and number of employees.

With our available inputs, there are several ways to project future workforce needs; and (ISC)² used a combination of three methods to estimate the size of the current cybersecurity workforce:

1. **Estimate the U.S. workforce represented by cybersecurity professionals.** This is a population-based average. We estimate the percentage of labor workforce cybersecurity professionals represented per U.S. state. This calculation includes the current workforce size (based on U.S. Census data) multiplied by the percentage of the expected cybersecurity workforce (based on the survey). On average, cybersecurity professionals represent 0.46% of the market's total workforce, with the U.S. range per state being 0.19% to 3.66%. For every 1 million U.S. workers, we expect to find approximately 4,600 cybersecurity professionals.

2. **Estimate the average U.S. headcount of cybersecurity professionals per business entity.** This is also a population-based average, but with a different numeric output. Per U.S. state, we estimate the average number of cybersecurity professionals per U.S. business entity. The calculation includes total U.S. business establishments (based on U.S. Census data) multiplied by the expected cybersecurity headcount per establishment (based on the survey). On average, there will be 0.103 cybersecurity professionals per single U.S. business entity. For every 100,000 U.S. business establishments, we expect approximately 10,300 cybersecurity professionals.

3. **Expand the average headcount of cybersecurity professionals across other countries.** This was a survey-based formulation to determine aggregate estimates per country by leveraging ratios observed from robust calculations based on U.S. data.

Results from all three calculation methods were statistically pooled to reduce potential noise from any single calculation. By combining and averaging figures from those three methods, we were able to estimate a current workforce of 879,157 individuals in the U.S.

After finalizing the calculation process for the U.S., given the availability of robust market inputs, we then applied the same process to 13 other countries where sufficient survey data was available: Canada, Mexico, Brazil, the U.K., Ireland, France, Germany, Spain, the Netherlands, Australia, Japan, Singapore and South Korea.

Notably, China and India were omitted from the calculation due to the limited information available about the size of the business sector in these markets. Because India and China have extremely large populations, and have been experiencing rapid economic growth, including these nations in our workforce estimation would introduce the potential to vastly overstate the cybersecurity professional population.

This estimation of the current size of the cybersecurity workforce provides useful context to help ground our findings, but there are other important considerations when interpreting these estimates:

International limitations: The availability of census data to provide a total count of businesses for any individual country outside of the U.S. is extremely limited, and few secondary sources are publicly available that accurately tally the total number of operating businesses internationally. Our estimate uses U.S. staffing ratios conservatively to extrapolate cybersecurity workforce populations outside of the U.S.; however, we recognize that U.S. business dynamics and staffing models may not apply directly to international markets. Given this lack of secondary data sources for some regions, the size of the current global cybersecurity workforce should be considered our best estimate.

Correcting for micro-businesses: Organizations with 1 to 50 employees are prevalent across all countries, but many of them do not employ their own technical staff or dedicated cybersecurity professionals. As a result, we have applied a correction factor within this company size range, to avoid over-representing the current number of cybersecurity professionals. This helps provide a more conservative estimate of the cybersecurity workforce.

The impact of COVID-19: Organizations both public and private have faced upheaval this year due to COVID-19. Rapid changes in revenues and operations mean that the survey results reflect a period of unprecedented uncertainty.

How the Cybersecurity Workforce Looks in 2020

It's no surprise that the industry that employs the most cybersecurity professionals in 2020 is the IT services industry. Again, as expected, this is a well-educated section of the population, with bachelors and master's degrees being the norm. Most of these degrees were in the STEM fields of Computer and Information Sciences and Engineering.

STUDY PARTICIPANTS

Geographic Distribution

Company Size Distribution

17%
1–99 employees

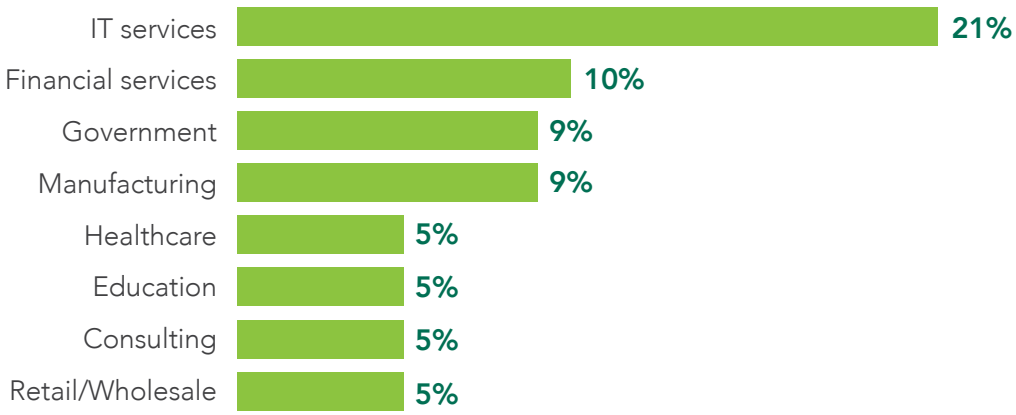
20%
100–499 employees

26%
500–2,499 employees

36%
2,500+ employees

Industries Distribution

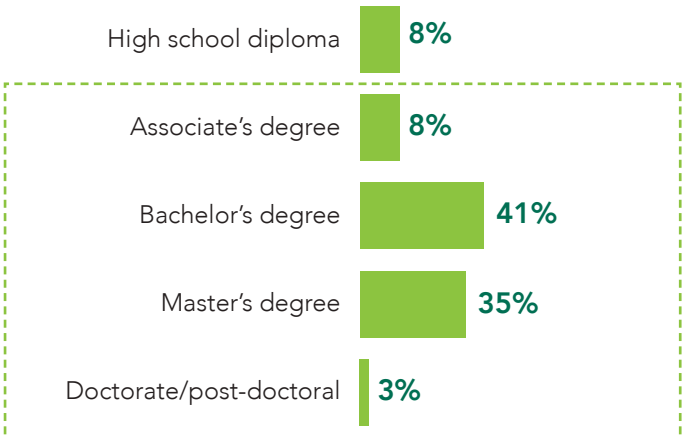
Cybersecurity professionals protect organizations around the world in a broad range of organizational types and sizes.



What Do Cybersecurity Professionals Look Like?

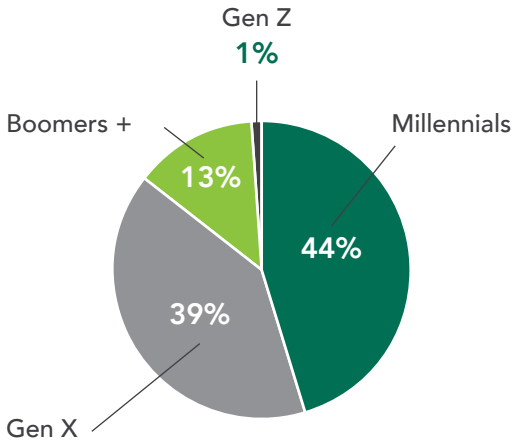
Cybersecurity personnel represent a wide range of educational backgrounds and ages, working in a broad range of industries and organization types. Most participants (72%) are male, and the largest age cohort is Millennials.

EDUCATION



Computer and information sciences: **49%**
Engineering: **20%**
Business: **10%**

AGE



Our survey included not only those with formal cybersecurity titles and full-time security responsibilities, but also IT professionals whose job includes a substantial portion—more than 25%—dedicated to cybersecurity tasks.

Titles Held

Cybersecurity is a shared responsibility across organizations, which is evident by the diverse array of job titles of survey participants that include formal cybersecurity roles, as well as IT positions. Titles held include:

- Application Developer/ Tester
- CIO
- CISO
- CTO
- Help Desk Technician
- Information System Security Manager (ISSM)
- IT Auditor
- IT Director
- IT Manager
- IT Security Director
- IT Security Manager
- IT Specialist
- Network/System Administrator
- Owner/CEO/President
- Security Administrator
- Security Analyst
- Security Architect/Engineer
- Security/Compliance Officer
- Security Consultant/Advisor
- Security Specialist
- Systems Architect
- Systems Engineer
- Technical Consultant
- VP IT

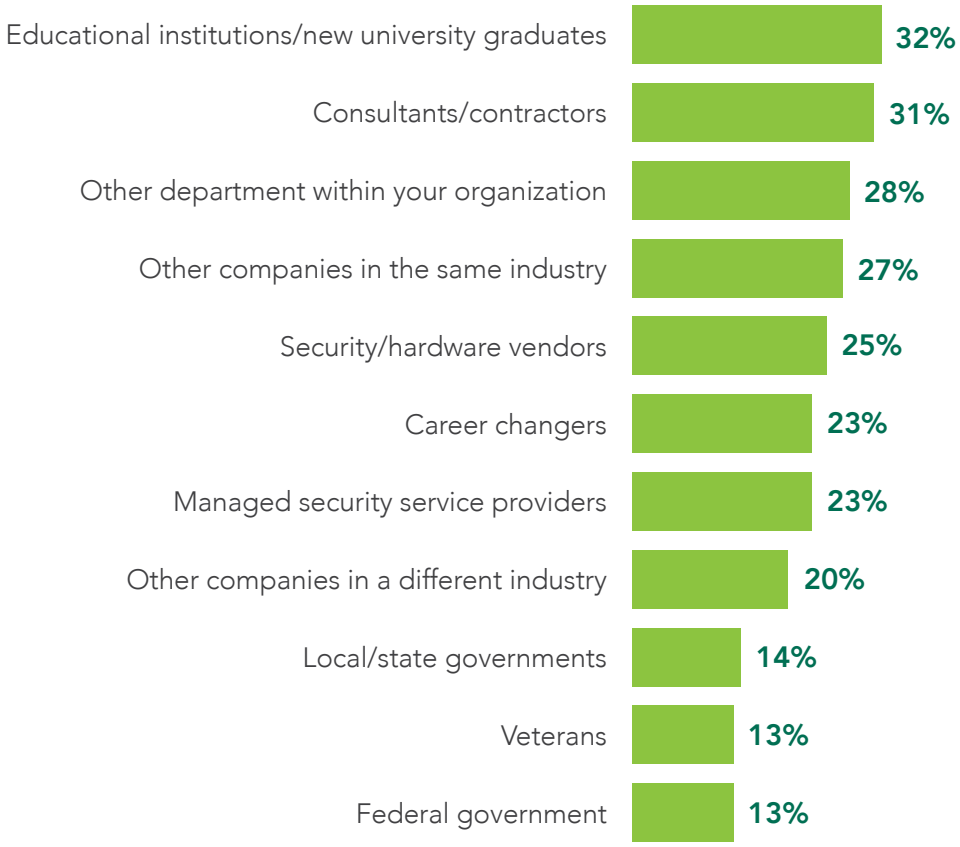
79% of cybersecurity professionals hold at least a bachelor's degree—with a little more than one-third holding a master's, doctoral or post-doctoral degree. While most in the field get their degrees in computer and information sciences (49%), others sought degrees that are not IT-focused, such as engineering (20%) and business (10%). Not to be overlooked is that 8% of cybersecurity professionals report holding only a high school diploma, illustrating that university degrees are not the only successful pathway into the field.

As for where hiring managers are finding candidates, organizations in Latin America and the Asia-Pacific region are more likely than others to recruit from educational institutions and security or hardware vendors, while organizations in North America and Europe are more likely than others to recruit consultants.

There are many possible paths to cybersecurity. A list of top recruiting sources as revealed by survey responses illustrates many of them, including recruitment of staff from other departments (utilized by 28% of organizations) and other companies in the same industry (27%) or from a different industry entirely (20%). Vendors in the security or hardware industries (25%) and career changers (23%) make the list as well.

Top Sources of New Cybersecurity Talent

The competition for skilled cybersecurity is widespread as organizations will reach out to a variety of sources to find the right talent.



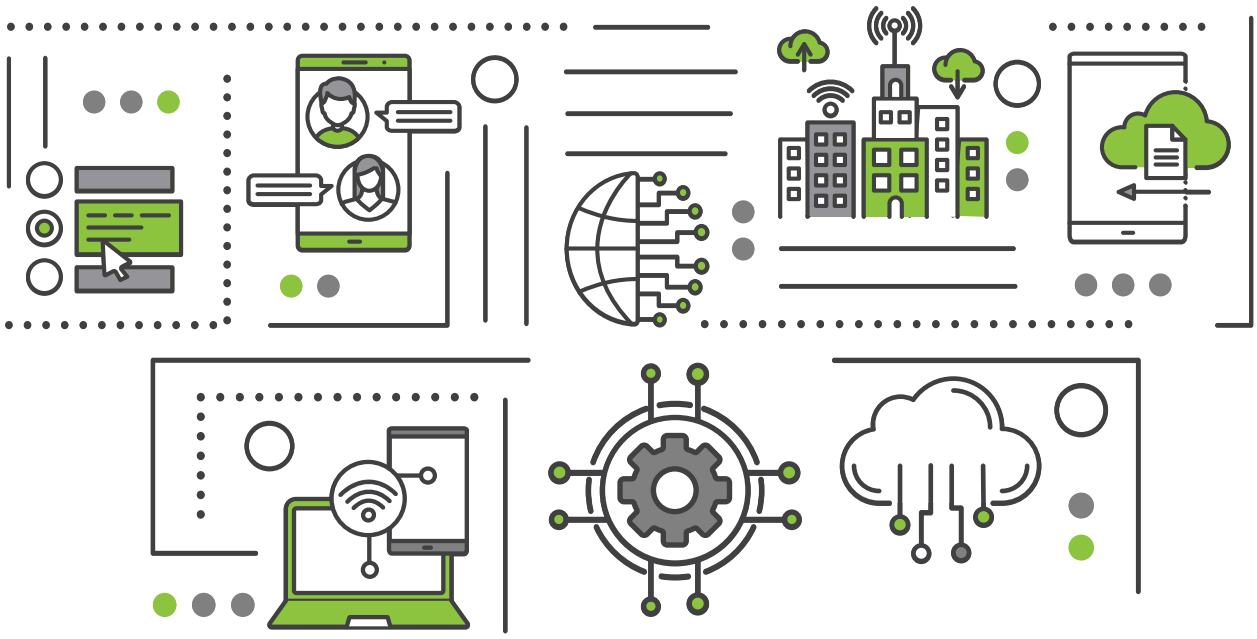
A Closer Look at Cybersecurity Professionals

Cybersecurity professionals tend to be both long-tenured and highly experienced. Survey respondents report an average of 11.5 years in an IT role, with 6.7 years at their current organization and 6.5 years in a cybersecurity role.

Cybersecurity Roles and Functions

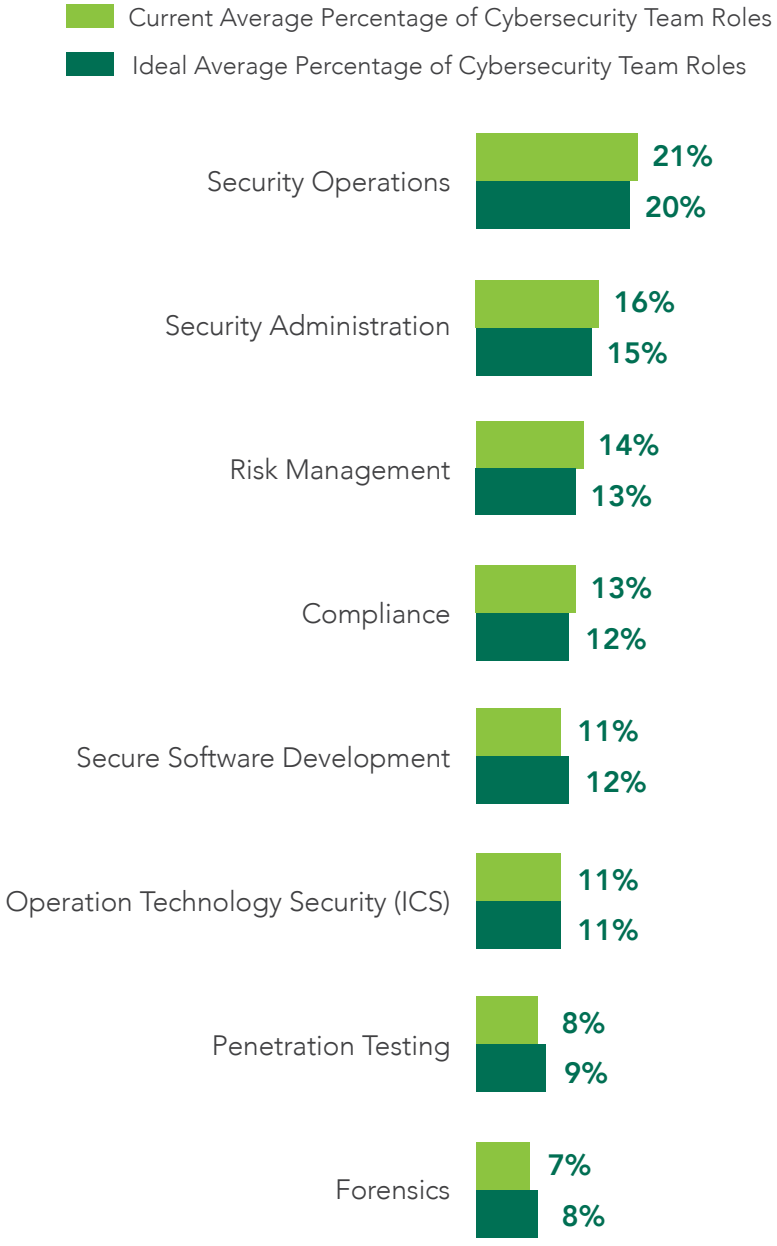
As this year has made clear, security is a widely shared task: not every cybersecurity role has the term "cybersecurity" in its name.

Titles aside, our research finds that organizations are distributing key roles and responsibilities across their cybersecurity teams in a way that closely aligns with respondents' ideal team structures. For the top three team roles by percentage within organizational cybersecurity teams—security operations, security administration and risk management—the actual distribution of roles was within a single percentage point of what respondents described as ideal. Even beyond those top three, the actual to ideal distribution remained closely aligned.



Cybersecurity Team Roles

Real-world team role allocation in cybersecurity aligns closely with what current professionals describe as ideal.

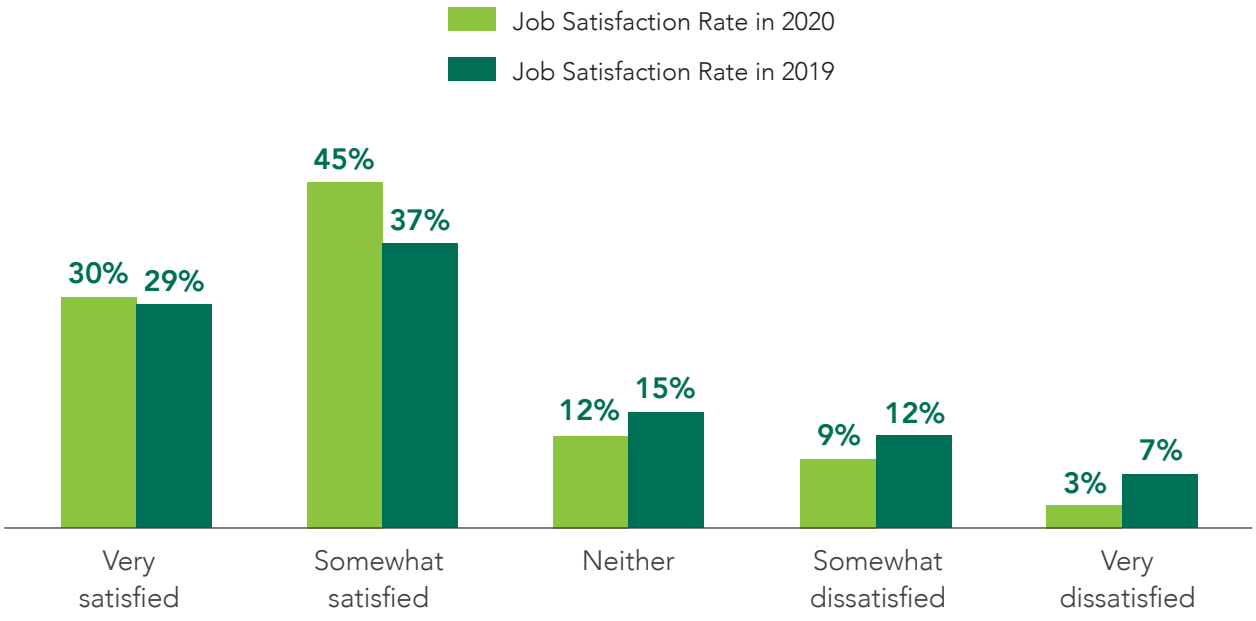


Job satisfaction among cybersecurity practitioners is extraordinarily high, despite a popular conception that security work is underappreciated and stressful. Job satisfaction in the field is at the highest level it has been for several years.

Worldwide, 76% (79% in North America—representing an increase over last year's figure of 71%) report that they are satisfied with their jobs, and just 12% overall report that they are dissatisfied in their current positions, which is just slightly less than last year's results, despite the added stresses and demands of responding to COVID-19.

Job Satisfaction Rates – Year-Over-Year

Job satisfaction among cybersecurity professionals is remarkably high—higher than it has been in several years.

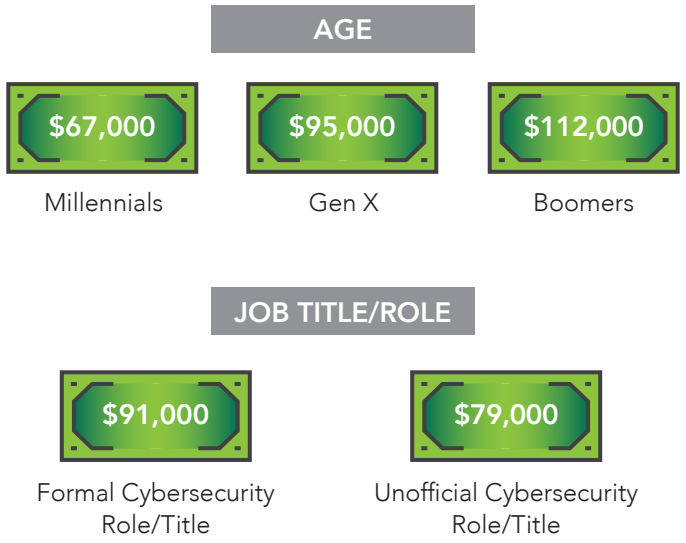


While job stability and compelling work are important contributors to job satisfaction, both job seekers and current professionals seek pay commensurate with their experience and the importance of the position they hold.

Cybersecurity professionals make about U.S. $83,000 per year, on average. The average salary is highest in North America ($112,000) and lowest in LATAM ($27,000), with APAC ($56,000) and Europe ($74,000) falling in between. Those holding security certifications have an average salary of $85,000 while those without earn much less—about $67,000, on average.

Salaries also vary by age, and according to whether an employee has a security-focused or IT-focused title. For Millennial professionals early in their careers, the average salary is $67,000. Employees with greater work experience enjoy higher salaries, with Gen X respondents reporting an average salary of $95,000, and those in the Baby Boomer generation reporting $112,000.

Cybersecurity Salaries Vary Across Age and Position Type



WHAT "CONSULTANT" MEANS IN TODAY'S CYBERSECURITY LANDSCAPE

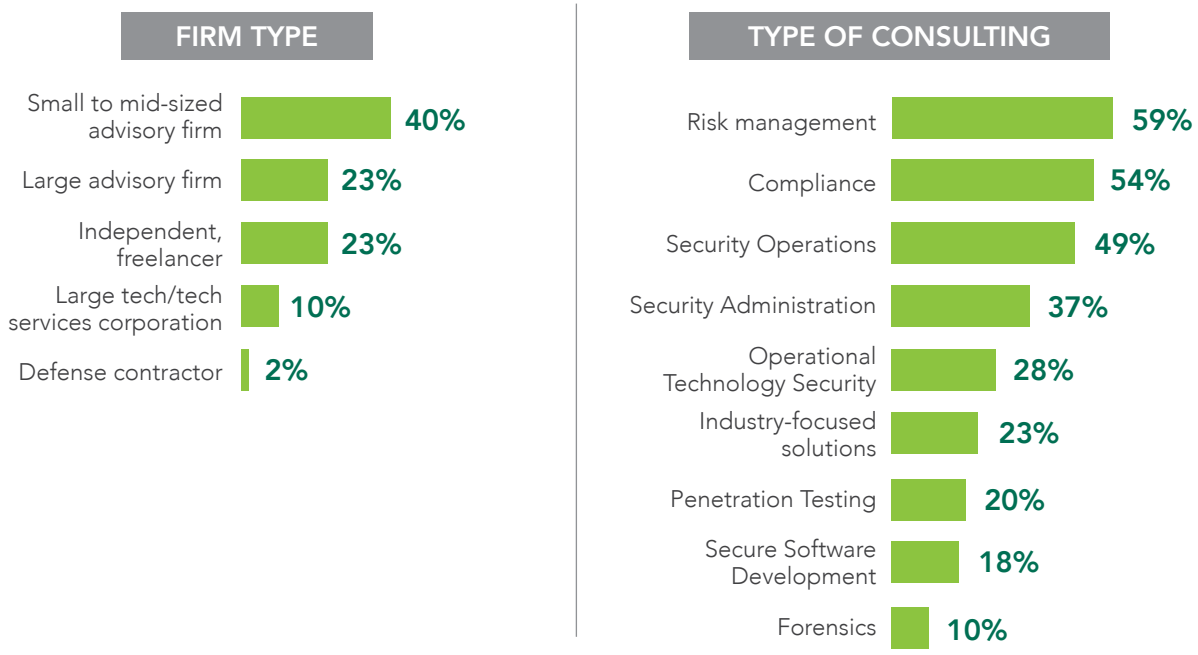
Even in a field where titles can be famously ambiguous, many respondents identify themselves as a "consultant." This year, for the first time, we asked respondents who identify as consultants to help us understand what this term means to them, and where they work.

Among our surveyed population, the largest group of self-identified consultants work for small to mid-sized (40%) firms, while 23% work for large advisory firms; 23% identify as independents or freelancers, 10% work for large technology or technology services providers, and 2% are employed by defense contractors.

Asked what type of consulting they engage in, respondents reported risk management (59%), compliance (54%) and security operations (49%) at the top of the list; beyond these three, the professionals in our survey most frequently reported working on security administration (37%), operational technology security (28%) and industry-focused solutions (23%).

Consultant Demographics by Firm Type and Type of Consulting Work

Cybersecurity professionals who serve as consultants work in a wide range of environments and across many varieties of consulting.



Why Certification Matters

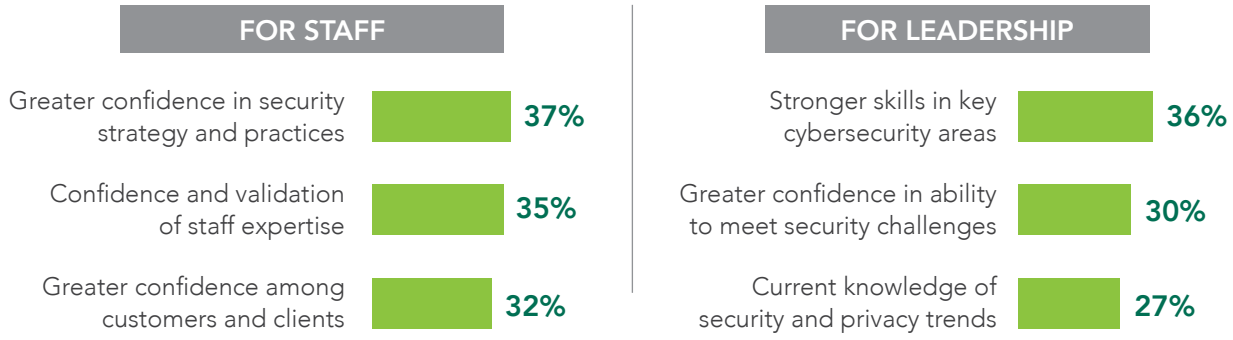
Building or being part of a robust team means supporting employees at all stages—from recruitment to professional development. One way for organizations to provide this kind of support is by contributing to (wholly or in part) employees' continuing education, including certifications.

Most cybersecurity professionals (63% worldwide) are currently pursuing or planning to pursue some sort of security-related certification within the next year. Certificates are seen as critical to professional and career growth. This is one reason why many cybersecurity professionals earn multiple certifications throughout their careers.

Employers value certified cybersecurity professionals for a number of reasons, from having increased confidence in strategies and practices (37%) to communicating and demonstrating that confidence and competence to customers (32%).

Other benefits of certification cited by employers include reducing the impact of a security breach, knowing that technology and best practices are up to date, and enhancing the organization's reputation within its given industry.

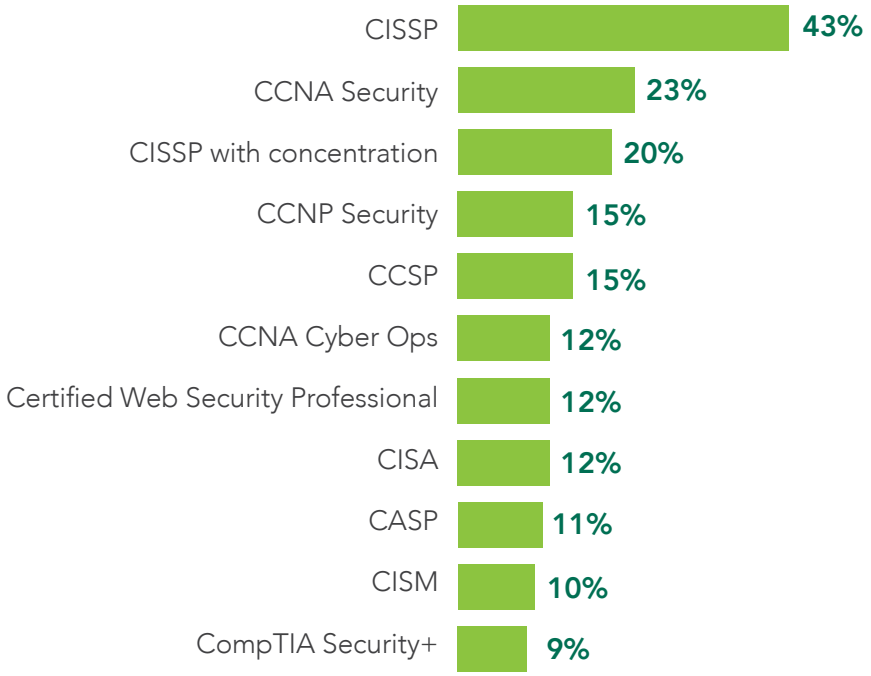
Top 3 Benefits of Cybersecurity Certificates



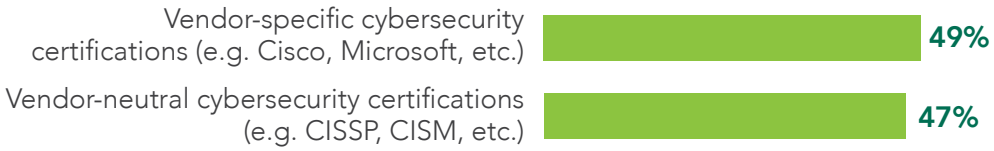
It's common, though not universal, for organizations to contribute toward certification-related costs. One reason for that may be changing workplace expectations. More than 70% of U.S. cybersecurity professionals say they are required to have some kind of certification, and the figure is even higher—78%—worldwide. Another reason to pay or subsidize employees' certification expenses might simply be for a workplace to be competitive in attracting and retaining a limited number of skilled applicants.

Security Certifications Held by Respondents

Cybersecurity professionals typically hold multiple vendor-specific and vendor-neutral certifications. These are the most commonly held among respondents.



Types of Certifications Employers Require

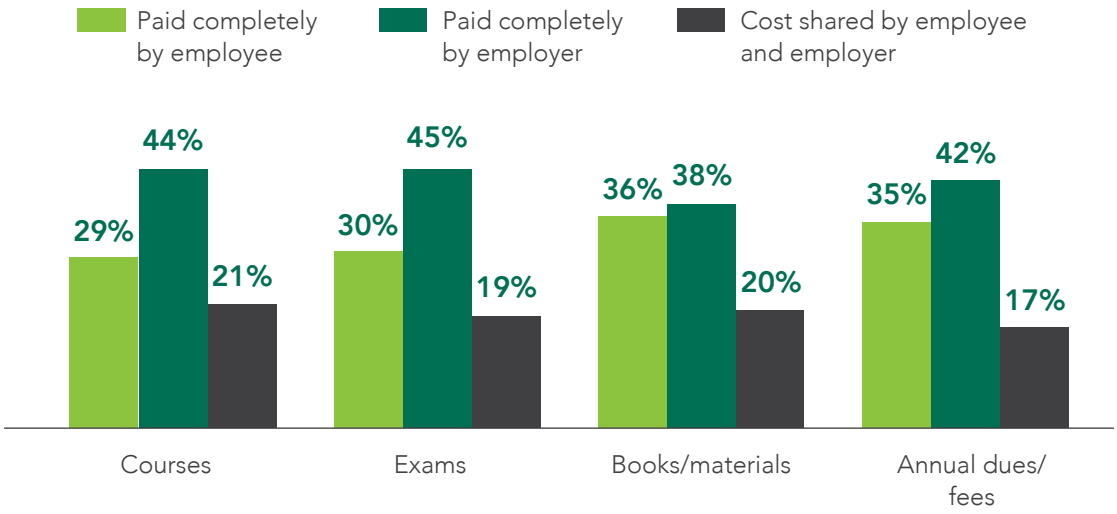


The role of employers varies. Respondents in Europe report the highest level of organizational support, with 50% reporting that certification courses, along with exam fees (51%), are paid for completely by their employers. In both Latin America and Asia-Pacific, however, just 41% and 40% of respondents, respectively, say their exams are fully paid for by their employers, along with 42% and 39% of related courses.

By bearing the cost of certifications, organizations can help keep their cybersecurity professionals satisfied, and make clear their value to the organization. This increases the possibility that these professionals will remain in their current positions while enabling cybersecurity teams to grow professionally.

How Organizations Contribute to Certification Costs

Employer contributions to employees' security certification costs vary widely; more than 40% of respondents report that their organization pays for courses, exams, and annual dues or fees.

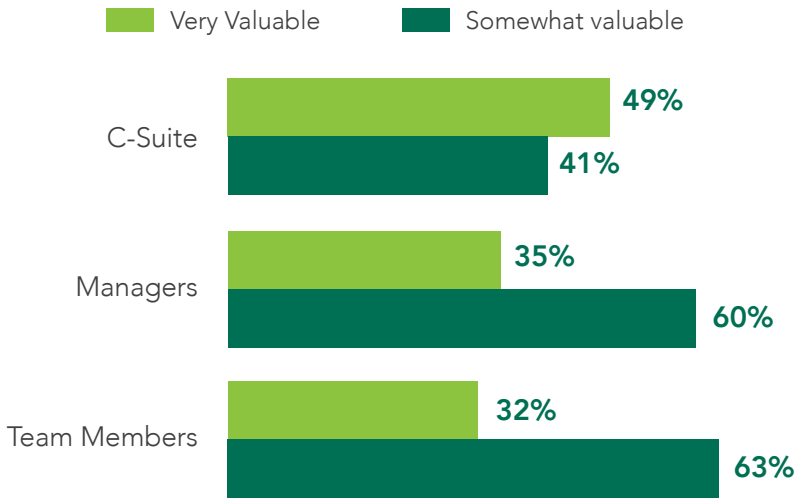


Respondents whose organizations pick up the tab for certifications display significantly higher job satisfaction rates than their peers who aren't as fortunate. As of last year, 72% of respondents whose certification costs were paid for say they are either very or somewhat satisfied with their jobs. That's compared to 63% of respondents whose organizations pay for only part—or none—of their certification costs.

Cybersecurity professionals find value not just in holding certifications themselves, but also in knowing that their colleagues and managers have accrued the same kind of knowledge that these credentials certify. Security competence is increasingly seen as vital not just for staff in the cybersecurity trenches, but increasingly for managers and even senior executives.

Cybersecurity Certification Value for the C-Suite, Managers and Team Members

Nine out of 10 cybersecurity practitioners see value in security certifications for C-suite executives, and even more see them as valuable for managers and other team members.



The Skills Cybersecurity Professionals Are Seeking

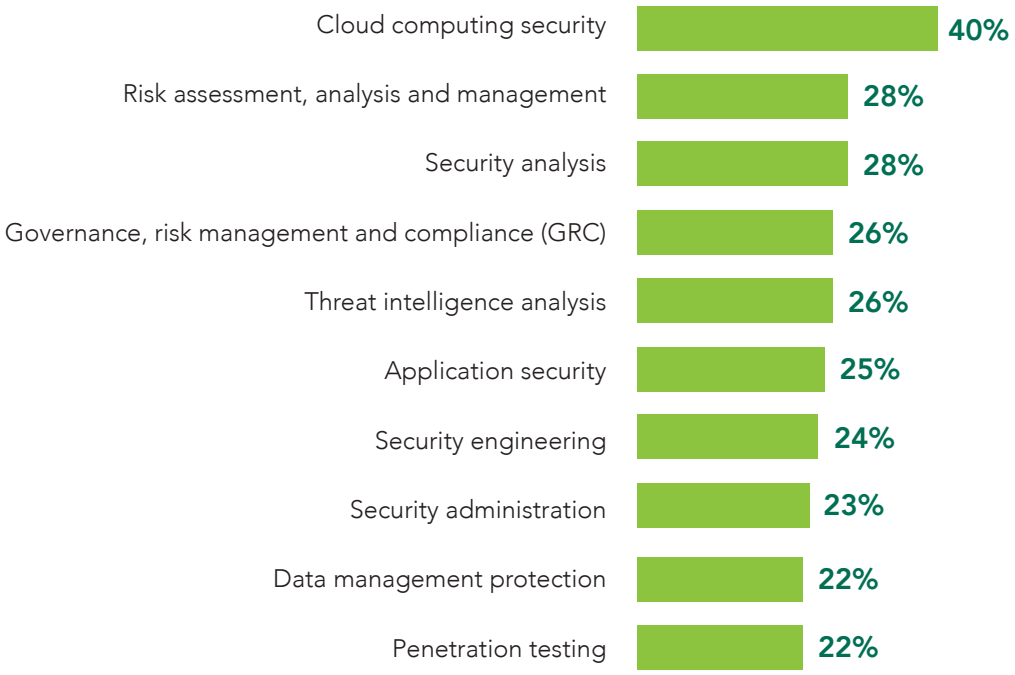
One reason that certifications are important, and why cybersecurity professionals seek them out, is to demonstrate their expertise as technology changes and industry trends emerge. A good example: remote work requirements have greatly increased the adoption and importance of securing the cloud.

While the cloud is not new, cloud services remain a challenge to secure. It's no surprise then, that 40% of cybersecurity professionals across roles, age brackets and company sizes named cloud security as the skill they most need to develop in the next two years, and no doubt an area in which they would seek to demonstrate their knowledge through certifications.

Other top skills that professionals have on their two-year horizon include risk assessment, analysis and management (28%); security analysis (28%); and governance, risk management and compliance (26%).

Top Cybersecurity Skills Needed

Cybersecurity professionals plan to develop their skills across multiple areas over the next two years, with 40% specifically naming cloud computing security as an area of focus.



"Preparation is key; don't underestimate the need to train and educate staff about security threats."

– Study participant

Women in The Cybersecurity Workforce—Perception and Opportunity

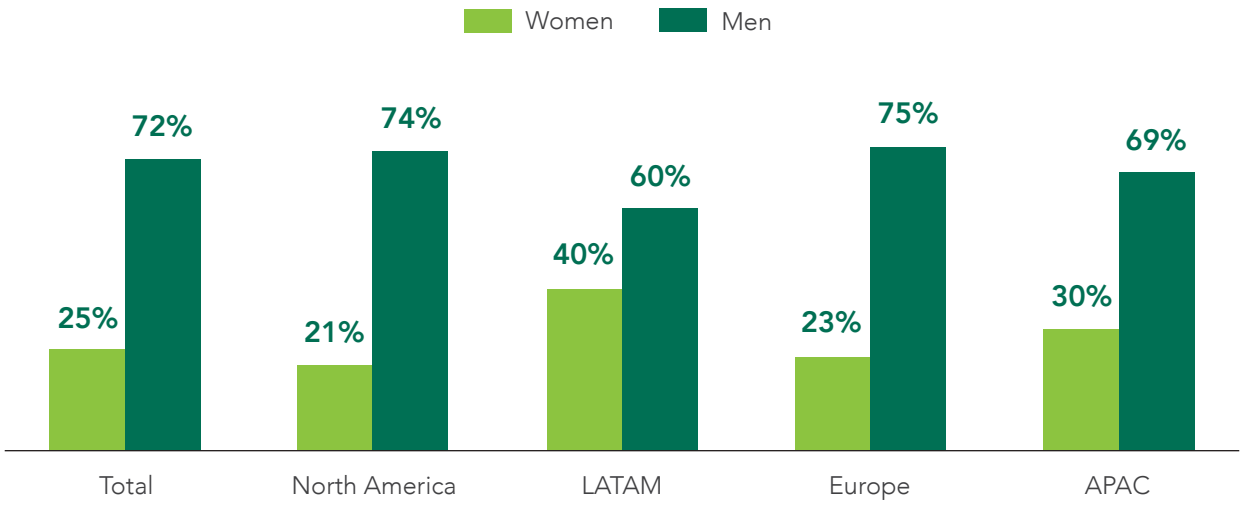
Cybersecurity professionals participating in our study are more than twice as likely to be men than women, meaning there is an underutilized pool of talent available.

Just over half of the surveyed cybersecurity professionals (51% worldwide, among both men and women) perceive the percentage of women in the field to have risen over the last five years. Among women, however, 7% view the number of women in the field to have actually declined in that time, compared to just 4% of men.

There are also large variations globally in this perception, with just 44% of European respondents saying that women's security workforce participation has risen, and 49% saying instead that it has remained the same or declined, while 65% of Latin American respondents reported a perceived increase. Our data, however, suggests that the actual percentage of women in the cybersecurity workplace has remained close to constant over the last three years, with women making up approximately 25% of our study participants.

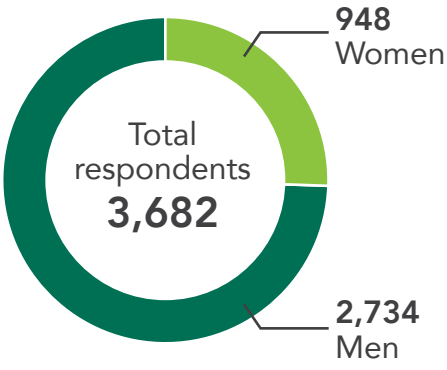
Whatever trends develop, in today's cybersecurity workforce, gender disparities are evident in every region; the highest percentage of women cybersecurity professionals participating in our study is in Latin America, with 40%, while in North America the figure is just 21%, and results in Europe and Asia-Pacific fall between these respective ranges, at 23% and 30%.

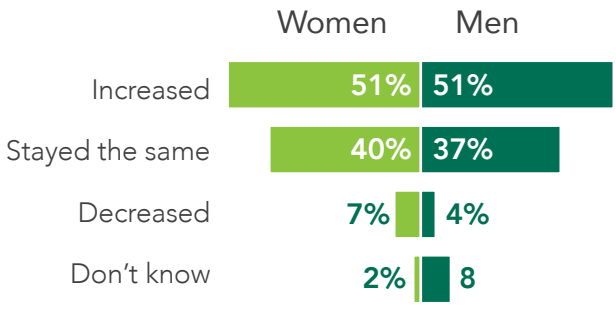
Breakdown of Study Participants by Gender



Perception of Women's Presence in the Cybersecurity Profession in the Last 5 Years

While just over half of all respondents say they perceive an increase in women in cybersecurity during the last five years, nearly twice as many women as men actually perceive a decline.





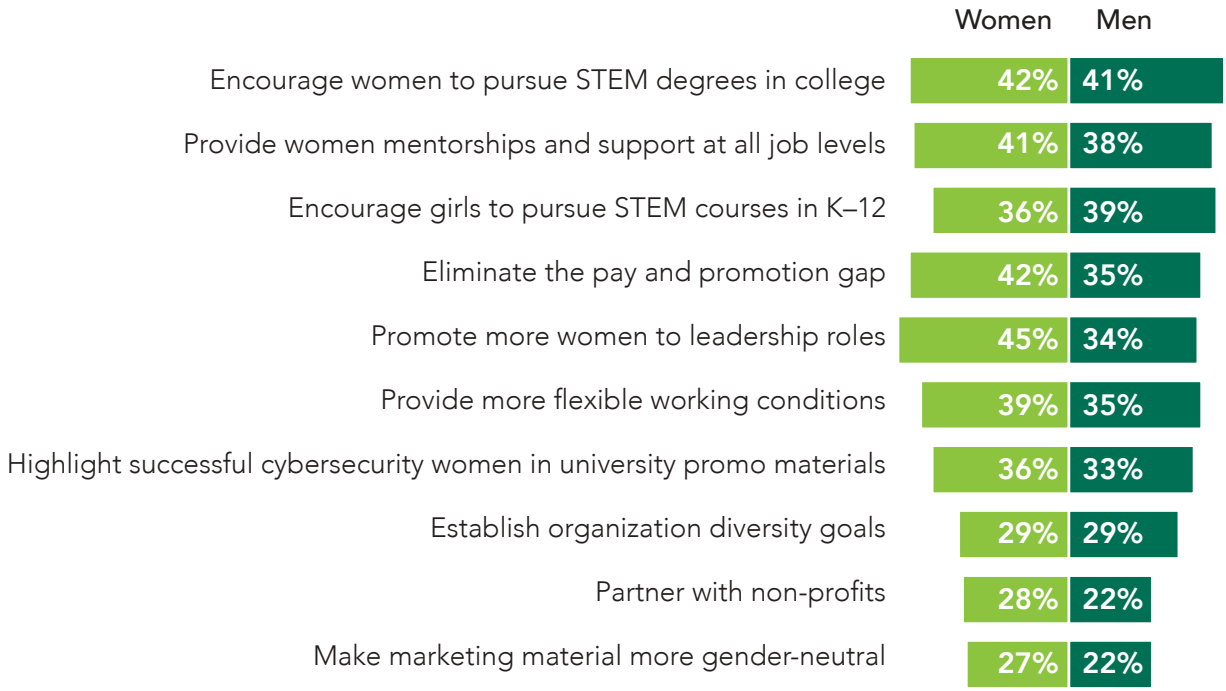
The gender disparity in cybersecurity represents an opportunity both for organizations to seek out and work to retain talented women applicants, and for women themselves to join a stable, growing and fulfilling profession.

42% of women and 41% of men among the respondents said the best way to increase women's representation in the field was to encourage women to pursue STEM degrees in college. Nearly as many said the same of providing mentorship and support to women at all job levels (41% and 38%, respectively).

Women also named, in far higher numbers than men, other strategies to help address the underrepresentation of women, including promoting more women to leadership roles (45%, compared to 34% of men) and eliminating the pay and promotion gap (42%, compared to 35% of men).

Top Ways to Increase Representation of Women in Cybersecurity

Both men and women cited education, recruitment and mentoring as valuable tools for increasing the presence of women in cybersecurity; women respondents also called to reduce disparities in pay, promotion and leadership presence.



Strengthening Your Cybersecurity Team in 2020 and Beyond

In a year dominated by COVID-19, organizations should ensure they recognize and appreciate the value that cybersecurity teams have already shown—and realize that there is much more to be done. As work from home continues, enterprise networks now extend to employees' homes, and threat actors will try to take advantage. Investing in your cybersecurity personnel is the best way to reward the value they provide.

As we have seen, 49% of respondents expect their organizations to hire more cybersecurity professionals within the next year. This is critical to organizations, as those that lack satisfied cybersecurity personnel are more likely to:

Have a significant cybersecurity staff shortage

Feel they are more vulnerable to cyberattacks

Have a poor security response to COVID-19-related issues

Even with management expecting tighter budgets in 2021, make sure you don't overlook the people who make the systems and solutions run. You need people to manage all that new technology. Pay attention to the things that make your workplace welcoming and rewarding, from simple collegiality to support for continuing education and professional growth.

The cybersecurity workforce gap is shrinking, but it persists. This demands that organizations be creative about how they fill roles and build their bench strength. Make your organization appealing by highlighting the opportunities and benefits you offer applicants, from on-the-job training to professional development and a path to advancement for all genders.

Consider non-traditional candidates, from career-changers to liberal arts graduates to ex-military personnel; the broader your net, the more potential candidates you can identify. Further opening the space, consider more work-from-home options for your cybersecurity workforce, as most professionals are learning to be just as productive and as effective working from home. This dramatically widens your available talent pool and may help attract more non-traditional candidates to your organization.

Look to certifications and the value they provide to your organization or professional development. In a profession with so many entry points, certifications help demonstrate and validate skill and experience. Moreover, they can be used to keep employees engaged and satisfied. Contributing fully or partially toward the cost of certification is a sure-fire way to keep staff satisfied and attract new and ambitious talent.

Keep in mind the skills that are most relevant and in-demand for your team. Help team members stay sharp, especially in cloud security. Maintaining a cybersecurity team for the long-haul means retaining employees, and job satisfaction is a key factor in retaining staffers in a competitive field. Commit to career-long learning opportunities that will help maintain the expertise of your team.

Conclusion

This year's study provides deeper insights into the state of the cybersecurity workforce at a time of unprecedented and rapid change, uncovering both the real-world security challenges that organizations face, and ways they can improve their cybersecurity readiness. It also highlights the importance of cybersecurity itself, with security competence increasingly an expectation not just for those with day-to-day security responsibilities, but at managerial and executive levels as well.

Despite both an ongoing pandemic and the tremendous, persistent global workforce gap that this report details, much of what we found is encouraging. Strong teams can thrive in the face of crisis, and today's cybersecurity professionals have had remarkable success in addressing security incidents even while helping to rapidly transform the workplace.

Our respondents were unambiguous in their support for recruiting more qualified cybersecurity professionals, as 56% say their organizations are at risk due to cybersecurity staff shortage. Putting together an effective cybersecurity team cannot be viewed merely as an option for any modern enterprise anymore. Building more robust cybersecurity teams is the imperative for 2020 and beyond.

For organizations that want to maintain their momentum, it's important that they keep their long-term, senior-level cybersecurity professionals satisfied and eager to share their deep institutional memory. They also need to continue to recruit a new stream of younger professionals interested in learning from their peers, and offering diverse new perspectives on maintaining the highest level of cybersecurity.

Employment in the field needs to grow by approximately 41% in the U.S., and 89% worldwide, to meet the anticipated demand. That growth is achievable, but it will require organizations to cultivate new professionals by looking beyond the current population of cybersecurity professionals, and prospecting for non-traditional employees, or career-switchers with non-traditional paths to cybersecurity positions, along with supporting their requirement for continuous learning and professional growth.

About (ISC)²

(ISC)² is an international nonprofit membership association which has focused for more than three decades on inspiring a safe and secure cyber world through education and skill-based certification. 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 membership, more than 150,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry.

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, better understand the barriers facing the cybersecurity profession, and uncover solutions that position these talented individuals to excel in their profession, better secure their organizations' critical assets and achieve their career goals.

Learn more at www.isc2.org/research.