(ISC)²

A Resilient Cybersecurity Profession Charts the Path Forward

(ISC)² CYBERSECURITY WORKFORCE STUDY, 2021

Table of Contents

Introduction

The 2021 (ISC)² Cybersecurity Workforce Study collected survey data from a record 4,753 cybersecurity professionals working with small, medium and large organizations throughout North America, Europe, Latin America (LATAM) and Asia-Pacific (APAC). Our findings shed new light on how the lingering effects of the pandemic and the accelerated evolution of the threat landscape impact organizations' security practices and the role cybersecurity professionals play in defending our critical assets.

For the third year running, the study provides two critical measures of the cybersecurity profession—the Cybersecurity Workforce Estimate and the Cybersecurity Workforce Gap.

The Cybersecurity Workforce Estimate presents an appraisal of the available pool of cybersecurity professionals worldwide. For 2021, our study estimates there are 4.19 million cybersecurity professionals worldwide, which is an increase of more than 700,000 compared to last year.

By contrast, the Cybersecurity Workforce Gap is the number of additional professionals that organizations need to adequately defend their critical assets. For the second consecutive year, the Cybersecurity Workforce Gap has decreased, down to 2.72 million compared to 3.12 million last year.

Together, the Cybersecurity Workforce Estimate and Cybersecurity Workforce Gap suggest the global cybersecurity workforce needs to grow 65% to effectively defend organizations' critical assets.

This report will guide you through the key findings of this year's research, including what the gap means in practice for professionals, what their organizations are doing to compensate for the lack of skilled personnel, in what disciplines they lack the most talent, and what organizations are likely to do to recruit and retain workers in the coming years. We also explore how professionals are ensuring they keep their skills current, what traits they value most in new entrants to the field, their morale during the pandemic, and what the adoption of work-from-home (WFH) or work-from-anywhere (WFA) means for them.

A Growing, Engaged Workforce

To protect their systems, employees and data, organizations around the world draw on a widely distributed pool of professionals. Study participants serve at all levels within their organizations, and hold titles that include Security Administrator, Security Analyst, Security Architect, IT Manager, IT Director, IT Security Manager, IT Specialist, CISO and CIO.

To quantify how many people are responsible for their organizations' cybersecurity, (ISC)² introduced the Global Cybersecurity Workforce Estimate in 2019. Unique to (ISC)², this global estimate integrates knowledge gleaned from thousands of survey respondents and an array of secondary data sources to extrapolate the number of people working to secure data, systems, infrastructure, privacy, vital services and more around the world.

Our Global Cybersecurity Workforce Estimate for 2021 is 4.19 million, a year-over-year increase of more than 700,000—a positive development during a period of global economic uncertainty. Who are these people and what do they look like? Our study sheds light on today's workforce.

"With an increase in remote work opportunities, and an increase in the frequency of cyberattacks, more cybersecurity professionals will have the ability to become employed with organizations who will utilize their abilities to the fullest extent."

– Study participant

The Cybersecurity Workforce Around the World (Number of Cybersecurity Professionals)

In addition to our global Cybersecurity Workforce Estimate of 4.19 million, our study provides 14 country-specific workforce estimates.

In 2021, we saw the most growth in

Germany
165% increase

Singapore
61% increase

United States
30% increase

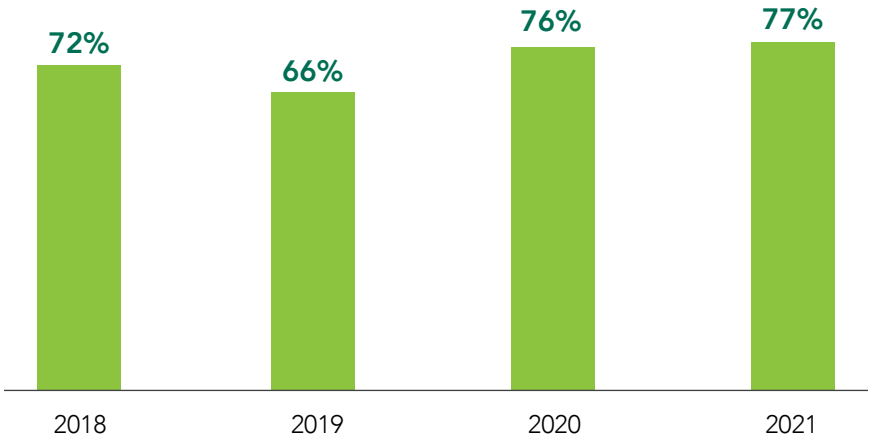
	2019	2020	2021
NA	**888,700**	**981,120**	**1,266,158**
U.S.	804,700	879,157	1,142,462
Canada	84,000	101,963	123,696
LATAM	**827,000**	**1,048,399**	**1,096,876**
Mexico	341,000	421,750	515,527
Brazil	486,000	626,650	581,349
EUROPE	**543,000**	**830,187**	**1,086,146**
U.K.	289,000	365,823	300,087
France	121,000	118,302	146,808
Germany	133,000	175,159	464,782
Ireland	N/A*	14,212	15,028
Spain	N/A*	122,284	124,336
Netherlands	N/A*	34,406	35,106
APAC	**544,000**	**625,265**	**743,075**
Australia	107,000	108,950	134,690
Japan	193,000	226,269	276,556
Singapore	43,000	57,765	92,744
South Korea	201,000	232,281	239,085
GLOBAL	**2,802,700**	**3,484,971**	**4,192,255**

* Country not included in estimate in 2019

Despite some of the prevailing narratives in the media about cybersecurity professionals feeling stressed, unappreciated and facing overwhelming pressure, our research continues to reveal a highly engaged and satisfied workforce.

Cybersecurity is anything but stable or predictable. Perhaps partly because of its very dynamism and the challenges it presents, many successful cybersecurity professionals overwhelmingly report happiness with their jobs. In fact, those currently in cybersecurity roles have consistently expressed very high levels of job satisfaction over the last four years, and they reported sharply higher satisfaction in the last two. For 2021, this includes the highest satisfaction figures ever reported. 77% of respondents reported they are satisfied or extremely satisfied with their jobs—significantly higher than the 66% reporting this level of satisfaction in 2019.

Strong Job Satisfaction for Cyber Pros
(Satisfied or Extremely Satisfied)

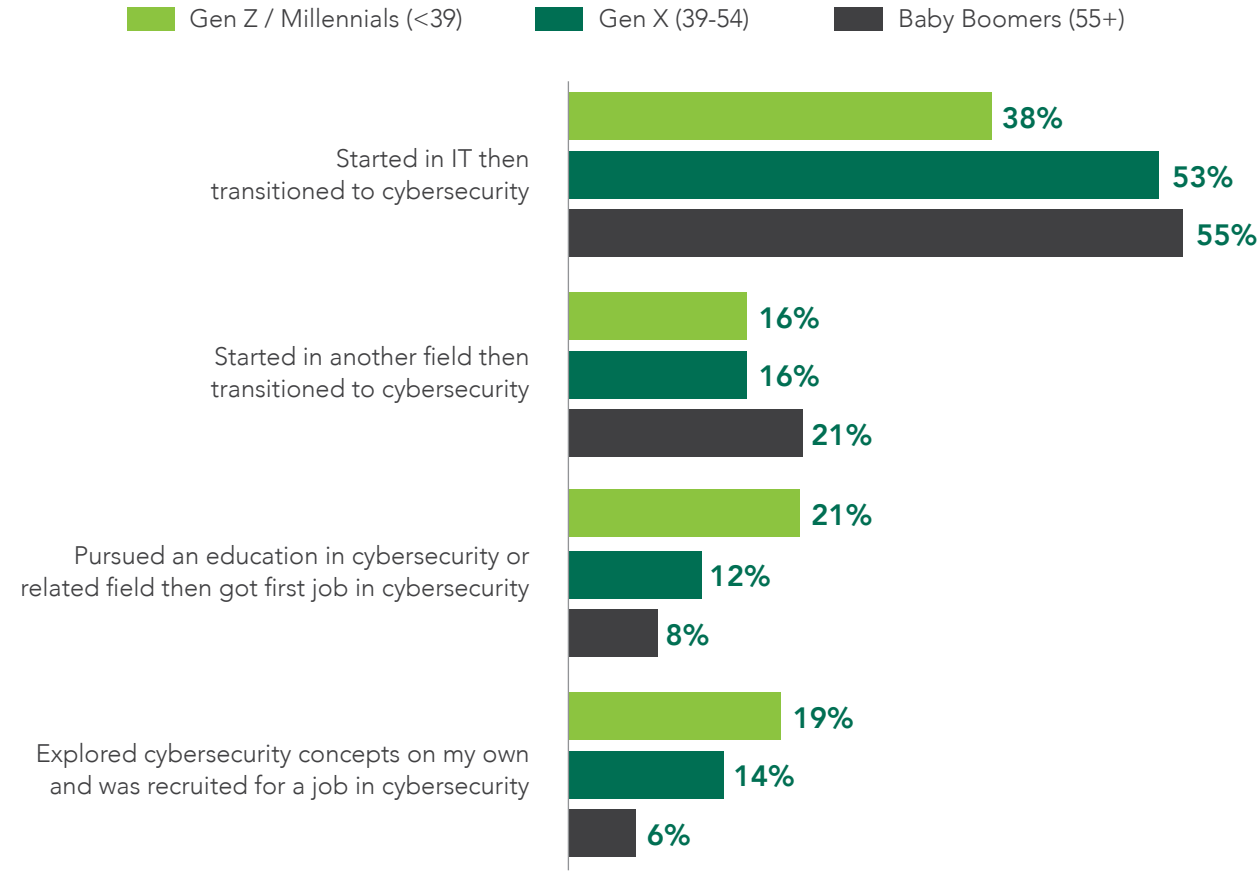


Job satisfaction among our study participants is highest among younger professionals (with 79% satisfied among Gen Z/Millennials) and only slightly decreases among Gen X (76%) and Baby Boomers (75%). Respondents working at mid-size and large organizations (500+ employees) are more satisfied than those at small businesses (less than 100 employees). And within industries, professionals working in retail had the highest satisfaction (83%) followed by manufacturing (82%), construction (81%) and IT services (80%). Those working in government (72%), telecom (72%), insurance (72%) and education (69%) had lower but still strong satisfaction rates.

Pathways to cybersecurity are changing. While an IT background remains the single most common route taken (47% of participants), that is giving way to a variety of entry points. Slightly more than half of cybersecurity professionals got their start outside of IT—17% transitioned from unrelated career fields, 15% gained access through cybersecurity education and 15% explored cybersecurity concepts on their own.

Getting a start outside of IT is more common for younger professionals. For Gen Z and Millennials, their pathways into cybersecurity are much more diverse than older generations. Only 38% started in IT, compared to 53% for Gen X and 55% for Boomers, and they have higher rates of entry through education and self-learning as well. This may indicate that cybersecurity is becoming better understood as a career opportunity for younger workers and students, but more effort is needed to ensure this broad and nuanced profession is less reliant on IT as the predominant pathway.

Pathways to Cybersecurity Careers



We also see a marked difference between men and women: fewer women (38%) came from an IT background than men (50%). Women have higher rates of entry from self-learning than men (20% vs. 14%) and pursuing cybersecurity education to land a job (20% vs. 13%). A similar trend is true for ethnic minority respondents: Black/African respondents (18%) and Hispanic/Latino respondents (22%) pursued education to land their first job at higher rates than Caucasian respondents (12%). *(Research note: Ethnicity and race were only asked of participants in the U.S. and U.K.)*

What Does the Global Cybersecurity Community Look Like?

With varied pathways to cybersecurity positions, it's hard to pin down what defines a typical cybersecurity professional. Our survey revealed in 2021 the global cybersecurity workforce is:

- Well-educated — 86% have a bachelor's degree or higher
- Technically grounded — among those respondents with college degrees, most graduated with degrees in STEM fields (46% computer science, 18% engineering, 3% mathematics) and some from business fields (8% business, 4% finance, 3% economics)
- Strongly compensated — respondents reported an average salary before taxes of U.S. $90,900—up from U.S. $83,000 among respondents in 2020, and U.S. $69,000 in 2019—with 31% reporting a median annual salary of U.S. $100,000 or more

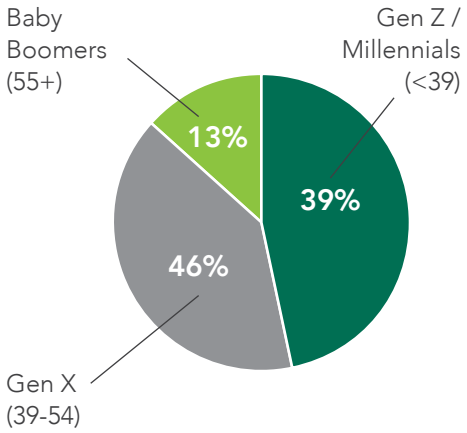
Salaries and their distributions vary broadly by region; notably, while only 9% of the North American workforce reported a pre-tax salary below U.S. $50,000, the largest single North American grouping (49%) earned more than U.S. $100,000. *(Research note: 26% of respondents globally chose not to disclose their salaries.)*

How Much Cyber Pros Earn Around the World (U.S. Dollars)

We also noted significant differences in average salaries between participants who have earned at least one cybersecurity certification compared to those who have not earned any certifications — those who have earned at least one certification made U.S. $33,000 more in annual salary than those that hold none.

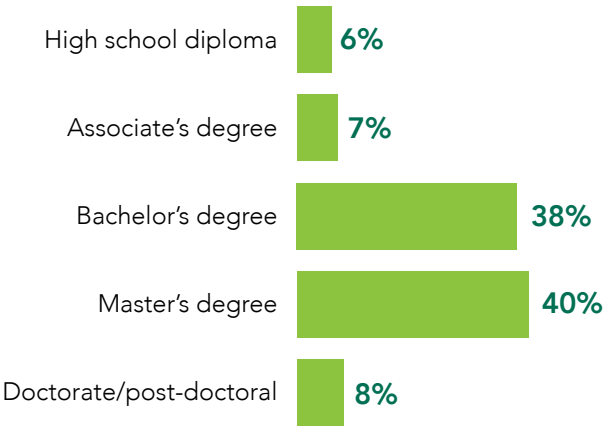
A Snapshot of the Cybersecurity Workforce in 2021

AGE



EDUCATION

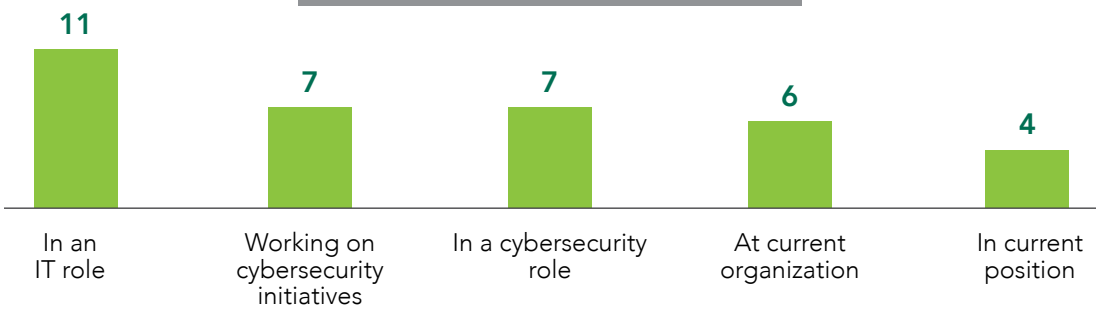
Highest Level of Education



Top Degrees

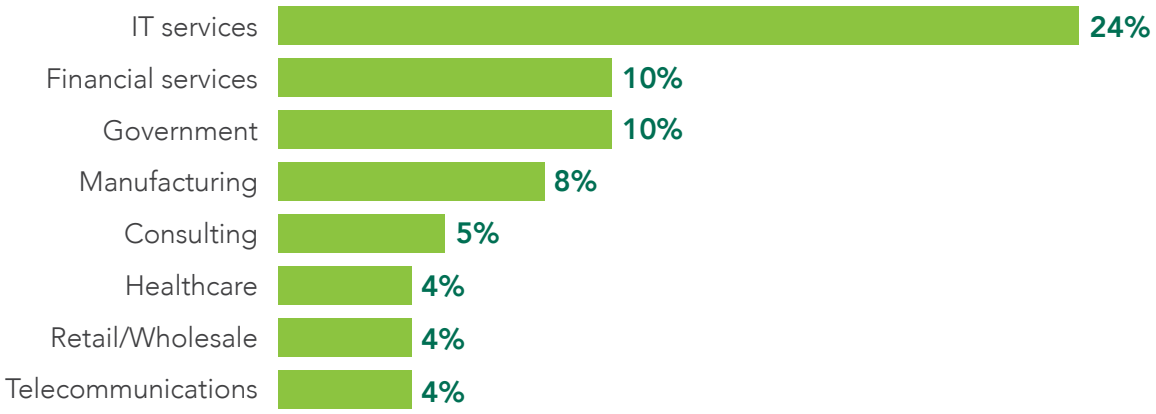
Computer and information sciences: **46%**
Engineering: **18%**
Business: **8%**

AVERAGE YEARS OF EXPERIENCE

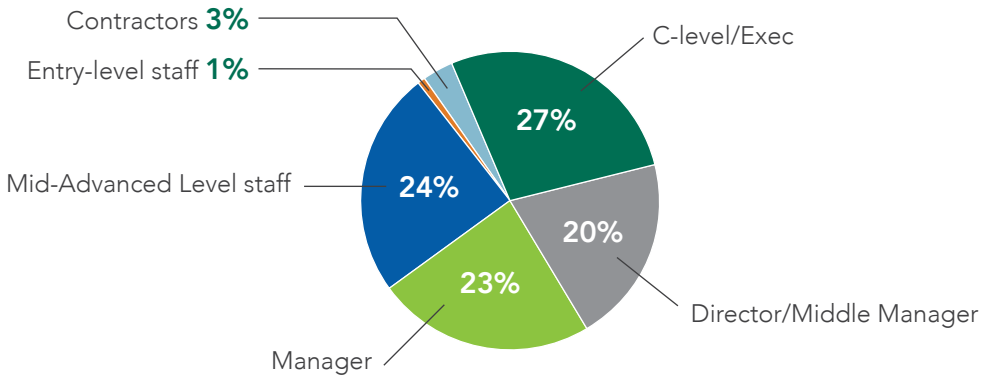


A SNAPSHOT OF THE CYBERSECURITY WORKFORCE IN 2021

Industry Distribution



Position Level



Company Size Distribution

15%
1–99 employees

19%
100–499 employees

26%
500–2,499 employees

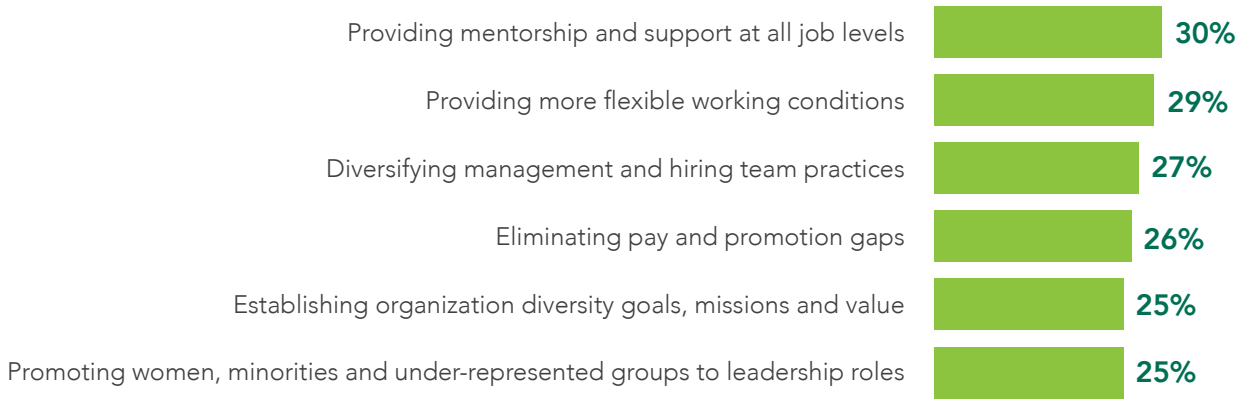
39%
2,500+ employees

Among study participants, the field also continues to be predominantly male (76%) and Caucasian (72%) in North America and the U.K. We observed a lower percentage of women among this year's study participants—20% overall—compared to 25% in 2020 and 30% in 2019.

Why did fewer women participate? Our study includes cybersecurity professionals in formal cybersecurity functions, as well as IT professionals who are responsible for cybersecurity operations at their organizations. This year, our response base included higher participation of professionals holding formal cybersecurity roles, which are more frequently held by men than women. Our data suggests a reliable estimate of women in the cybersecurity workforce globally remains at 25%.

How can Cybersecurity Diversify?

Study participants tell us it's a combination of initiatives.



Data also suggests that organizations are looking for a broader array of qualities in new recruits.

The Most Important Qualifications for Cybersecurity Professionals (Non-technical Skills and Attributes)

38%
Strong problem-solving abilities

32%
Curiosity and eagerness to learn

32%
Strong communication skills

23%
Strong strategic thinking skills

Many of these traits are now seen as equally important as cybersecurity certifications (32%) and relevant cybersecurity experience (31%).

A key takeaway for job seekers and managers alike is that people interested in cybersecurity roles should not need to rely on a lengthy checklist of technical skills, degrees and certifications to be considered for a role. Instead, the profession is actively looking for other valuable, non-technical talents new entrants can bring to the table. This added dimension of recruiting has the potential to greatly expand the talent pool for cybersecurity and increase the diversity of potential job candidates.

Top Attributes Sought in Cybersecurity Personnel

The growing importance of a broader mix of skills, both technical and non-technical, underscores the reality that today's cybersecurity roles are multi-dimensional and increasingly varied across specializations, organizations and industries. There are many different definitions and opinions of what a cybersecurity professional does.

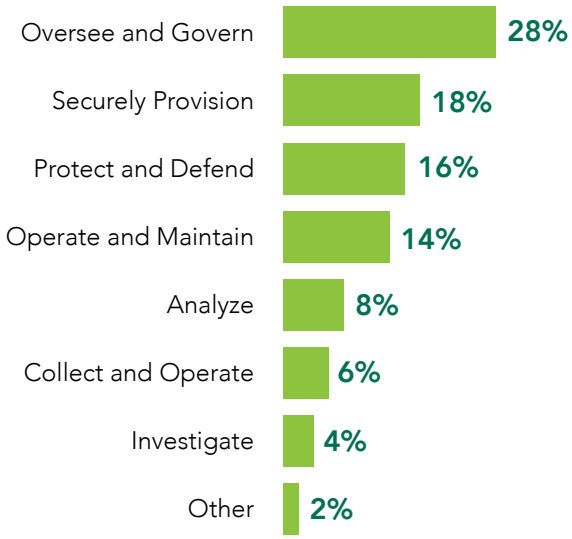
One way to apply a standard view of today's cybersecurity field is through the lens of the NICE Framework[1], which describes seven high-level groupings of common cybersecurity functions, more than 30 distinct areas of specialization and more than 50 detailed work roles. For the first time, our study reveals how the global workforce aligns with the NICE Framework. *(Research note: While the NICE Framework has recently evolved to de-emphasize these categories, it is constructive to compare the composition of the global cybersecurity workforce to the framework since it was introduced as a standard for government and the private sector.)*

The breakdown of the global cybersecurity workforce across the framework's seven high-level groupings shows that the largest percentage of the workforce globally (28%) identifies their primary role as falling under Oversee and Govern.

Oversee and Govern also is the most selected answer for cybersecurity professionals by age (Gen Z and Millennials: 22%; Gen X: 32%; Baby Boomers: 35%), gender (25% of men, 29% of women), and tenure (28% of respondents with more than four years on the job, as well as those with fewer). Similarly, Oversee and Govern is the most common role for professionals at organizations of all sizes, whether the participant holds a formal security title or not.

The remainder of the global cybersecurity workforce identifies their roles as Securely Provision (18%), Protect and Defend (16%), and Operate and Maintain (14%). Fewer than 10% of the cybersecurity professionals surveyed named any of the remaining NICE specialized framework categories – Analyze, Collect and Operate, or Investigate – as their primary role.

Where Cybersecurity Professionals Fit Within the NICE Framework



Cyber Pros Embrace Professional Development

The top five anticipated areas of investment in professional development highlight a blend of technical skills, such as artificial intelligence/machine learning (AI/ML) and threat intelligence, along with a mix of complementary skills (including risk analysis, security governance and compliance).

With continued emphasis on remote work, cloud security sits firmly as the top priority for cybersecurity professionals' skills development in the next two years, named by 40% of respondents just as it was in 2020.

Rounding out the top five areas for skills development were:

- Risk assessment, analysis and management (26%)
- Artificial intelligence/machine learning (25%)
- Governance, risk management and compliance (GRC) (24%)
- Threat intelligence analysis (22%)

Areas of focus do differ depending on participants' roles, age and the size of the company where they are employed.

Older professionals want to learn more about cloud computing than their younger peers, with 47% of Baby Boomers saying that cloud computing is the skill they need to cultivate most. Among Gen X, that number is 43%, and even lower (34%) among younger respondents. This may be attributable to older workers having developed their skills while securing and provisioning traditional data centers, while younger professionals may have come of age in the field over the last 10 to 15 years as cloud-first or hybrid IT infrastructures were being adopted.

Moreover, employees of larger organizations (500 employees or more) show a sharply higher desire to learn more about cloud security as well, with 43% of them naming it a desirable skill, compared to 34% of employees at small or medium (fewer than 500 employees) organizations.

Top Areas of Professional Development Participants are Pursuing

40%
Cloud computing security

26%
Risk assessment, analysis and management

25%
Artificial intelligence / machine learning

24%
Governance, risk management and compliance (GRC)

22%
Threat intelligence analysis

22%
DevSecOps

22%
Security engineering

21%
Security analysis

20%
Application security

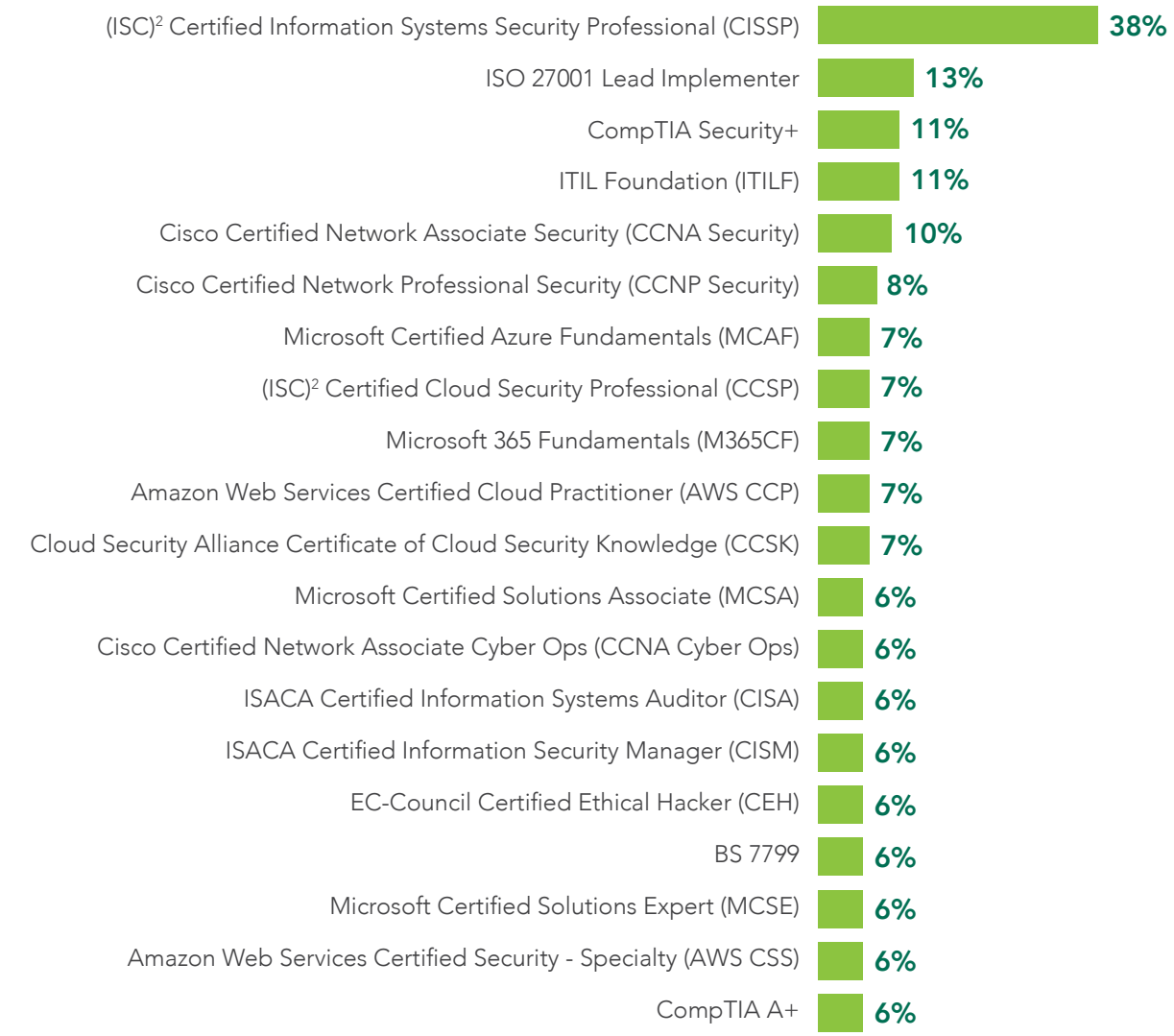
20%
Security administration

Professional Development Through Certifications

Nearly 50% of cybersecurity professionals are currently pursuing or planning to pursue certifications within the next 6 months, and just 11% say they have no plans to pursue certifications.

Why get certified? According to the study, 72% of cybersecurity professionals are required by their organization to earn certifications, with the demand almost evenly split between vendor-neutral certifications such as the CISSP and CISM, and vendor-specific certificates, such as those issued by Cisco and Microsoft.

Most Commonly Held Certifications and Certificates



Top Certifications and Certificates Being Pursued This Year

Benefits of Employing Certified Professionals

Study participants tell us certifications held by individuals create advantages and opportunities for the entire team. We asked survey participants to name the top benefits their teams realize from employing professionals with cybersecurity certifications. They named:

- Stronger knowledge in key cybersecurity areas (38%)
- Increased confidence in the team's handling of security challenges (30%)
- Higher-level personnel in-house with security expertise (27%)
- Staying up to date on the latest security and privacy trends (27%)

The impact of cybersecurity certifications extends beyond individual teams to the entire organization. Participants indicated that certifications helped their respective organizations:

- Validate security staff expertise for greater confidence (33%)
- Provide greater confidence in the organization's security strategy and practices (32%)
- Increase specialization and expertise in different cybersecurity areas (30%)
- Instill confidence in their ability to conduct secure transactions and processes (27%)

Top Value of Certification for Employers

Where Confidence and Validation of Staff Expertise Made the Most Impact

53%
Goverment (military)

44%
Goverment (non-military)

40%
Insurance

37%
Financial services

36%
Healthcare

33%
Telecom

31%
Software / hardware development

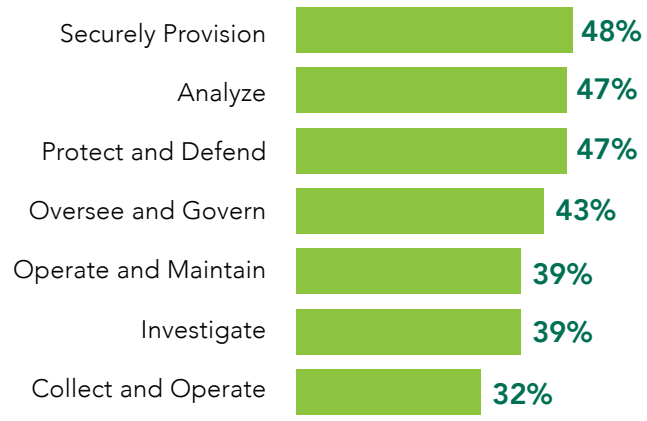
The Cybersecurity Workforce Gap

Our study was conducted in the wake of unprecedented nation-state compromises of the software supply chain[2], as well as surging ransomware attacks that crippled critical infrastructure[3] and disrupted vital services around the globe. At the same time, organizations were undergoing accelerated transformation during a worldwide pandemic. Still, cybersecurity professionals say the workforce gap remains the number-one barrier to meeting their security needs. Two-thirds (60%) of study participants report a cybersecurity staffing shortage is placing their organizations at risk.

Despite another influx of 700,000 professionals into the cybersecurity workforce, the 2021 study shows that global demand for cybersecurity professionals continues to outpace supply — resulting in the Cybersecurity Workforce Gap.

All areas of cybersecurity are affected by the staff shortage. Participants indicate staff shortages within their own organizations in each of the seven functional areas defined by the NICE Framework. The top cited categories of highest need were Securely Provision, at 48%, followed by Analyze, and Protect and Defend, each with 47% of participants saying they need more staff in these areas.

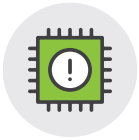
Cyber Staffing Shortages by Functional Area Worldwide



Real Consequences of Staff Shortage

32%
Misconfigured systems

30%
Not enough time for proper risk assessment and management



29%
Slow to patch critical systems

28%
Oversights in process and procedure

27%
Inability to remain aware of all threats active against our network

27%
Rushed deployments

Staff shortages have real-life, real-world consequences. What are the benefits of bridging the workforce gap? Would we really be more secure if we eliminated the gap?

To find out, we asked participants, for the first time, to share what negative impacts their organizations have experienced because of their own cybersecurity workforce shortages. The 2021 study confirms, from the perspective of the global cybersecurity workforce, that when cybersecurity staff is stretched thin, the negative consequences are real: misconfigured systems, slow patch cycles, rushed deployments, not enough time for proper risk assessment, not enough oversight of processes and procedures, and more. The list of issues cybersecurity professionals say can be prevented with enough people covers many root causes of reported data breaches and ransomware attacks.

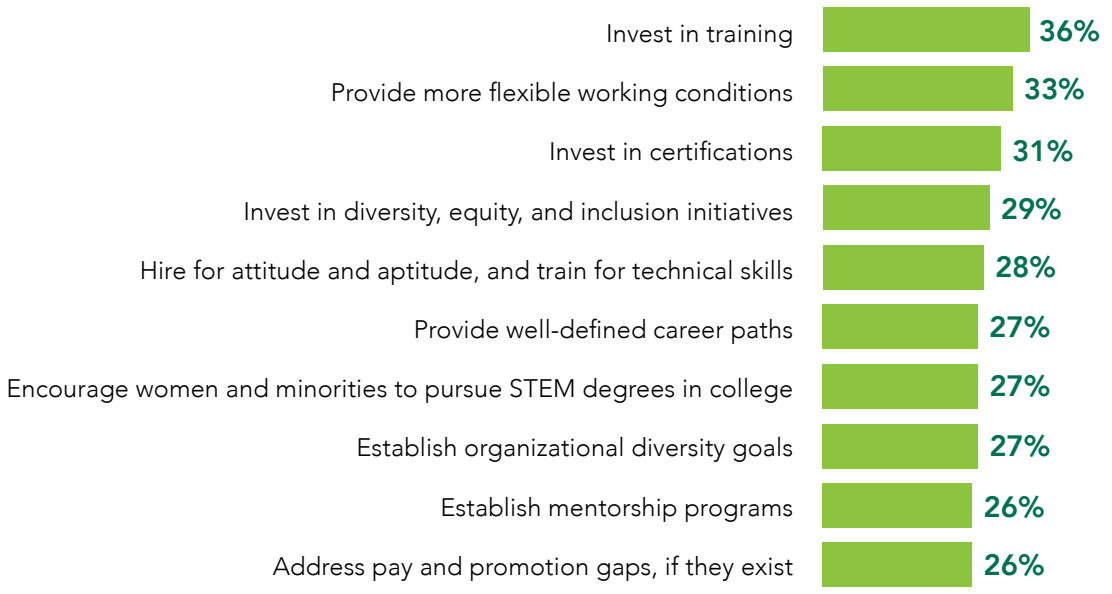
Addressing the Gap

Cybersecurity professionals suggest people-first approaches, complemented by process and technologies, are key to addressing the workforce gap.

With respect to people, participants placed by far the greatest emphasis on the development and retention of existing staff, with 42% of respondents globally naming it as having the greatest impact on shrinking the cybersecurity workforce gap. This was followed by initiatives aimed at recruiting new staff (31%) and encouraging the development of future staff (23%). 17% cited the use of AI/ML and automation in cybersecurity operations. This and other data signal that while important, cybersecurity professionals do not view technology investments alone as an adequate proxy for more people doing the work.

Asked what their organizations were planning to do within the next year to address their own cybersecurity workforce gaps, participants cited 10 areas of anticipated people-centered investments. Half of the activities—such as technical training and certification—apply generally to all cybersecurity personnel, but the remaining half directly support expanding their cybersecurity teams. The study also reveals that professionals expect their organizations to adopt new practices to foster alternative pathways into cybersecurity roles. This may enable them to tap into the talent of historically under-represented populations within the field.

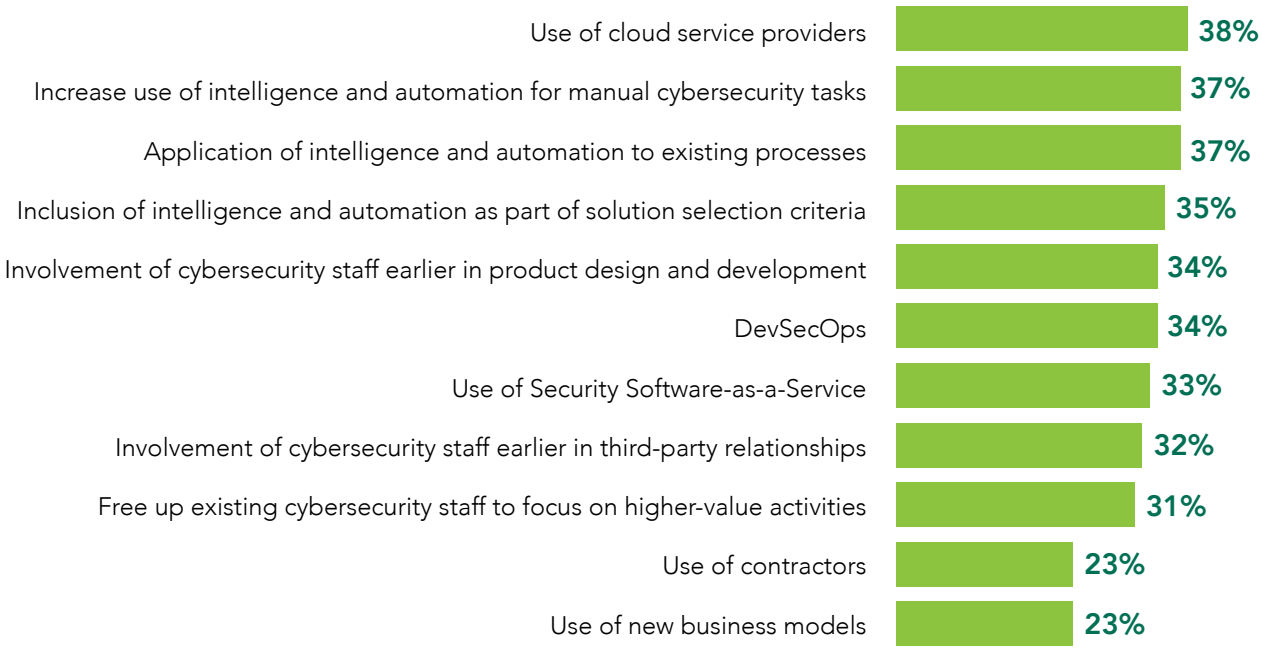
Top People Investments Organizations are Making to Address the Workforce Gap



> **"Moving up the stack—as we move to higher levels of abstraction (containers, serverless), we need to understand and partner much more closely with application developers to implement security earlier in the pipeline."**
>
> ***– Study participant***

Asked about how their organizations will invest in technology in the next year in response to their own workforce gap, participants anticipate increased use of cloud service providers (38%), increased use of intelligence and automation for manual cybersecurity tasks (37%), and applying intelligence and automation to existing processes (37%).

Top Technology Investments to Overcome the Gap



Imagine There's No Gap: Where Would You Invest?

How would cybersecurity professionals improve their security posture if their organization's personnel needs were fully met?

Four of the top five responses involve even greater investments in people: training and certifications (50%), professional development (46%), and automation solutions to make their tasks easier (48%). Additionally, 49% of respondents would invest in security awareness training for everyone in the organization.

Asked if a fully staffed cybersecurity team would enable them to divest of technology and security services, only one area (spending on third-party service providers like an MSSP) was cited by more than 10% of participants. This suggests that, even as their teams grow, cybersecurity professionals anticipate the need for continued technology and services investment to ensure they have the tools and support necessary to do their jobs and effectively strengthen their security posture.

The Global Cybersecurity Workforce Gap in Numbers

Besides an updated estimate of the size of the global cybersecurity workforce, a key objective of this study is to quantify the industry's workforce gap and uncover solutions for addressing the persistent talent shortage.

To calculate the gap, we apply a country-level data model that predicts the number of hiring organizations, estimates relative security team size by company size, and accounts for anticipated hiring demand for the year, survey responses and other factors. The result is our annual, point-in-time assessment of the Cybersecurity Workforce Gap. *(See more about our methodology on page 38.)*

For the second year in a row, we observed a narrowing of the global Cybersecurity Workforce Gap, from 3.1 million in 2020 to 2.7 million in 2021.

Our study estimates that 700,000 professionals joined the cybersecurity workforce in the last year; it is easy to draw the conclusion that the industry is making sustained progress toward closing the skills gap. However, a deeper dive into global trends behind the gap assessment suggests applying the brakes to that cautious optimism.

Gap in Cybersecurity Professionals Since 2019

Global ~2.72M	NA ~402,000	LATAM ~701,000	Europe ~199,000	APAC ~1.42M
Pandemic (2020): ~3.12M	Pandemic (2020): ~376,000	Pandemic (2020): ~527,000	Pandemic (2020): ~168,000	Pandemic (2020): ~2.045M
Pre-pandemic (2019): ~4.07M	Pre-pandemic (2019): ~561,000	Pre-pandemic (2019): ~600,000	Pre-pandemic (2019): ~291,000	Pre-pandemic (2019): ~2.6M

The gap in the cybersecurity workforce varies by region. We are seeing the workforce gap increasing in North America, Europe and LATAM. However, APAC countries show a continued decrease in the cybersecurity workforce gap. In fact, the continued decline is substantial enough to offset the demand in the rest of the world and effectively pull the global gap lower than our 2020 measurement.

The Global Cybersecurity Gap by Country (Number of Cybersecurity Professionals Needed)

In addition to the global Cybersecurity Workforce Gap estimate, our study provides a gap assessment for 14 countries.

It's important to note that APAC's declining workforce gap does not suggest a problem solved. With a remaining gap of more than 1.42 million, APAC employers are struggling to find qualified, skilled professionals.

The (ISC)² Cybersecurity Workforce Gap looks at both the number of hiring organizations, as well as how aggressive these organizations will be in their hiring practices. Many APAC economies and specific sectors within the region are reporting a slower economic recovery from the COVID-19 pandemic than North America and Europe[4], which may be due to global supply chain disruptions, slower COVID-19 vaccine rollouts[5] and sectors within the region being more vulnerable to uncertain global demand. Reports also suggest disproportionate numbers of APAC small and medium businesses (SMBs) going out of business due to the pandemic[6], as well as the relative strength of IT services providers (who support SMBs) as leading cybersecurity employers within the region.

Our data also show that cybersecurity hiring trends among APAC SMBs and mid-market organizations lag behind their global counterparts in intent to hire this year, suggesting ongoing relative softness in the cybersecurity. Larger APAC enterprise employers, however, have remained relatively steady in their hiring demand, already surpassing pre-pandemic levels when our survey was conducted.

Outside of APAC, we are seeing the Cybersecurity Workforce Gap continues to grow again alongside our Cybersecurity Workforce Estimate. This indicates that the need for more professionals in the field has never been greater, continuing to outpace demand and underscoring that career opportunities will only continue to grow.

"There will be huge security impacts in the coming year from the move to work from home (WFH) fueled by COVID-19. More attacks will occur on home computers and networks, with bad actors even using home offices as criminal hubs by taking advantage of unpatched systems and architecture weaknesses."

– Study participant

The Lasting Impact of the Pandemic

While nearly all study participants are currently employed, 29% of them temporarily left the workforce or experienced reduced hours at some point in 2020, with the top reasons globally being childcare (30%), furloughs (29%) and employers going out of business (29%). Additionally, 27% cited personal health reasons for leaving, while 17% cited family health reasons.

While the pandemic has brought its share of stresses, most cybersecurity professionals report that their personal morale during the pandemic has been above average (29%) or excellent (26%). Globally, 51% of respondents also described their teams' morale as above average (31%) or excellent (20%), and only 12% say that their personal morale has been below average or worse. Examining the global data by professional role shows even higher overall positive morale among those in manager (57%), director (56%) and C-level (67%) positions. A similar pattern is true for reported team morale during the pandemic.

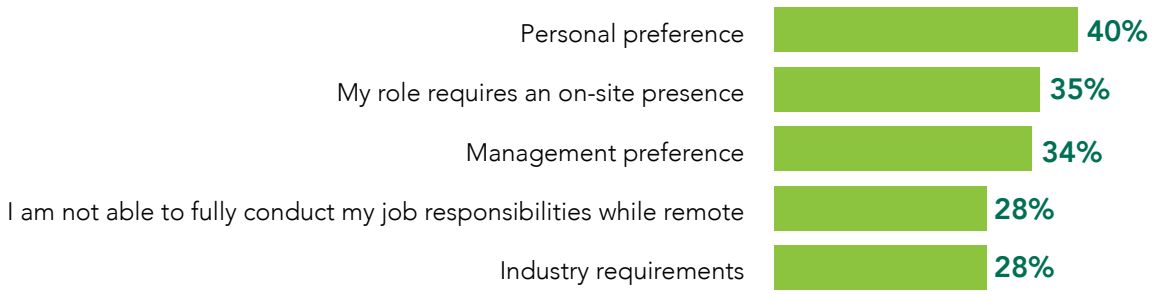
Our study found that while nearly the same percentage of cybersecurity professionals (about 85% globally) work remotely in 2021 as in 2020, a larger share of them this year (37%) must come to the office at times, which was true for only 31% in 2020.

There are also fewer fully remote employees now than there were in 2020 – 47% this year compared to 54% in 2020. The most drastic year-over-year changes are found in LATAM and APAC, shifting from 67% and 45% working fully remote in 2020, respectively, to just 48% and 36%.

Only 24% of companies across the globe have plans to fully return to a conventional office environment. And even less of the cybersecurity workforce—just 15%—want to fully return to an office.

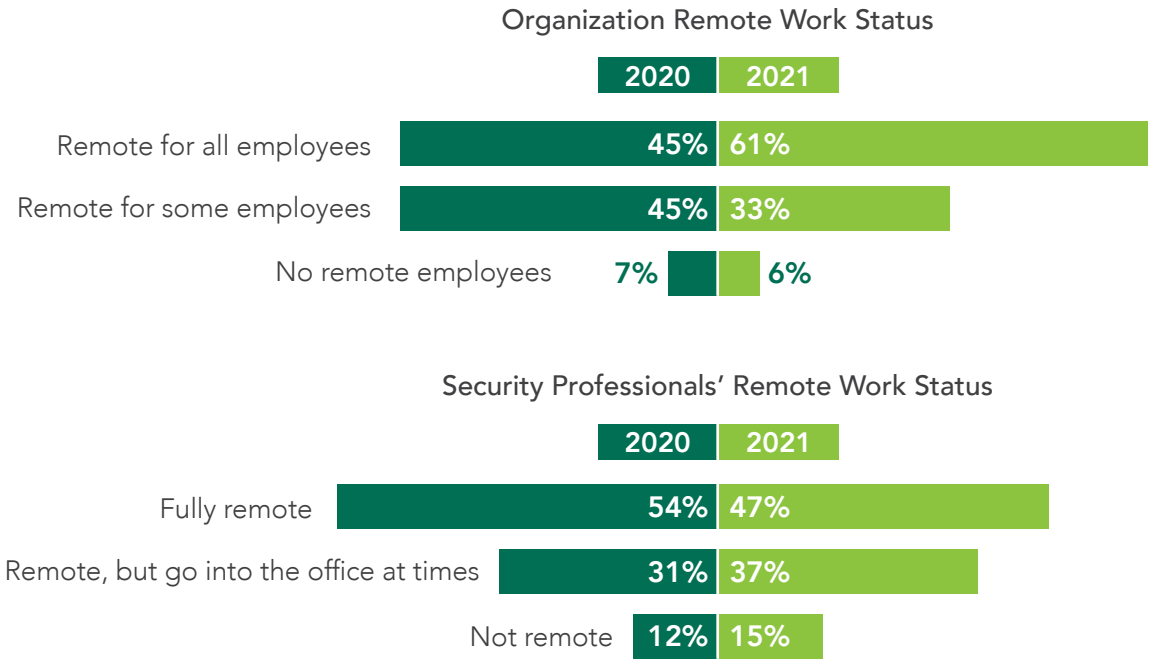
Since the previous study, more organizations have established WFH policies. This shows that companies are not only implementing WFH or WFA policies out of necessity for the safety of their workforce – they are also listening to employee preferences to remain remote.

Top Personal Drivers to Go into the Workplace



All indications are that the shift to remote work has changed the way people live and how organizations do business. By May 2020, 90% of participants' employers had implemented a WFH policy. Today, that number stands at 94%.

Implementation of WFH or WFA Policies



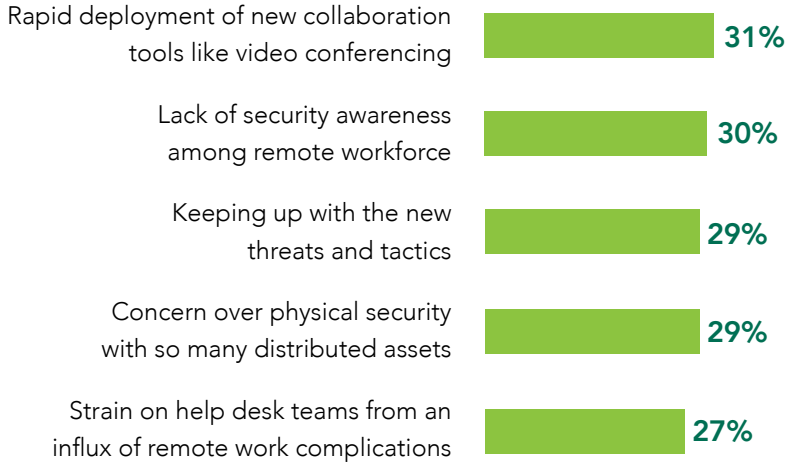
Besides the advantages of remote work as a public health measure, the rising number of companies with WFH/WFA policies reflects the positive experiences many organizations have had with a remote workforce, most notably, the continued productivity leaders have seen from their remote employees.

Cost reductions from consolidating or eliminating corporate workspaces have also impacted organizations' decisions. Where the sudden shift to working from home was a temporary necessity in 2020, in 2021 the benefits of a remote workforce have become solidified in many organizations. This trend also extends to the cybersecurity workforce. While these professionals may have likely been viewed as essential on-site personnel in the past, the last year has proven they can be successful working remotely.

Drivers for Organizations to Move to a Fully or Mostly Remote Workforce

However, the good news about remote work is offset by the challenges it is creating with an evolving threat landscape and multiplying attack surfaces. The tools that a remote workforce requires can put users and data at risk. 31% of respondents whose organizations have instituted a WFH/WFA policy for some or all of their employees name the rapid deployment of new collaboration tools, like video conferencing, as a challenge in keeping their remote workforce secure. Nearly as many (30%) say the same of a lack of security awareness among remote employees. Physical security matters, too: 29% describe physically securing widely distributed assets as a challenge. An equal number say they are challenged to keep up with new threats and tactics.

Challenges in Keeping the Remote Workforce Secure



Positive Change

The global pandemic has stressed organizations by disrupting supply chains, making it harder for employees to interact in person with customers and each other, and forcing greater use of remote collaboration technology. Nonetheless, participants named several ways in which the pandemic has changed their organizations for the better, citing improved workplace flexibility (53%), accelerated innovation and digital transformation efforts (37%), and stronger collaboration (34%) as just some of the unexpected ways the pandemic has spurred improvements.

How COVID-19 Responses Have Changed Organizations for the Better

Other less tangible but also significant improvements named by participants include strengthened organizational support for employees, a newly fostered common mission, and a sense that teams have been brought closer together, cited respectively by an impressive 29%, 23% and 22% of professionals globally.

Asked to name the areas their organizations need to address to improve security around the changes linked to COVID-19, respondents' top five answers included cloud infrastructure (45%), endpoint security (36%), application security (34%), mobile device management (33%) and a zero-trust security approach (32%).

The global business and technology landscape is undergoing massive transformation. Despite the daunting challenges presented during this upheaval, the cybersecurity workforce has adapted in real time, evolving through adversity, finding innovative solutions for moving forward as they fortify security for their respective organizations, and proactively prepare for whatever comes next.

"It's inevitable that we will see numerous security problems emerge in the cloud, if only because a shared cloud service becomes more unstable and unsecure as the demand increases. Organizations will need to ensure that they have developed security policies and guidelines for both public and private cloud use to mitigate the security risks."

– Study participant

Conclusion

The 2021 (ISC)² Cybersecurity Workforce Study is illuminating on many fronts.

First, it is exciting to see tremendous growth in the field to bolster defenses against new threats. More than 700,000 cybersecurity professionals joined the workforce despite the uncertain economic conditions created by the ongoing COVID-19 pandemic. Second, while we saw the talent gap rising in most regions, conditions in APAC contributed to an overall decline in the Cybersecurity Workforce Gap for the second year in a row. This underscores that the need for more cybersecurity professionals continues to outpace the growing pool of available talent, putting pressure and increased urgency on organizations around the world to find solutions.

Fortunately, this year's study participants have charted a course forward. The cybersecurity workforce – the very people on the front lines defending our critical assets around the world – are telling us where talent is needed most; that old habits in hiring need to change; that technology spending alone won't fix our problems; that remote work is a greater opportunity than a threat; and that they expect meaningful diversity, equity and inclusion (DEI) initiatives from their employers.

Understand Your Gap

Cybersecurity professionals told us how their day-to-day lives are impacted by the gap, and how real-world, avoidable consequences of not having enough staff leave organizations vulnerable. They unequivocally tell us that the lack of cybersecurity talent on their teams is their top concern. Using the NICE Framework, cybersecurity professionals told us in which high-level categories they needed the most help. While most participants say they work in roles that best align with Oversee and Govern, they tell us that more people are needed who work in roles within Securely Provision, Analyze, and Protect and Defend.

Takeaway: The insights gained from this year's study can help inform where recruiting efforts should focus. While needs are substantial across all skill categories, it is instructive to hear from cybersecurity professionals about where they see the most need. For individual organizations, hiring managers should consider where they have the largest talent gaps. Carefully craft roles and descriptions to address teams' specific needs, instead of overloading jobs with unrealistically broad responsibilities. Also, look to create growth opportunities, career pathways and cross-training. Build specializations around what your operation needs. Find opportunities to create roles that rely on critical and creative thinkers with enough technology-savvy to learn the role and contribute to your mission.

Rethink How You Hire

As previous (ISC)² research[7] revealed, cybersecurity professionals say a wide array of non-technical skills are critical for new entrants to succeed in the field. Traits they now say are equally or more important than certifications and relevant cybersecurity experience include strong problem-solving abilities, curiosity and eagerness to learn, strong communication skills, and strategic thinking. This shift away from a technology-first mindset is signaling a growing awareness that cybersecurity is much broader than the IT-centric environments where many long-time professionals gained their initial experience. Cybersecurity must be ingrained in processes, operations and strategies at all levels. And in uncertain, unpredictable environments, new perspectives and solutions are necessary.

Takeaway: Hiring organizations can significantly expand their pool of candidates if they start evaluating internal and external prospects for the non-technical skills and attributes professionals describe as vital for a successful cybersecurity career. Hire for aptitude and attitude. Recruit people from different backgrounds who are attracted to the challenges and rewards of a cybersecurity career and are willing to learn. This approach also immediately creates a more diverse pool of talent and can bring new and fresh perspectives to an operation.

Put People Before Technology

Study participants prioritize people investments before technology when it comes to strengthening their organization's security posture and addressing their own workforce gap. They tell us that organizations should prioritize the development and retention of existing staff, focus on recruitment, and encourage the development of future staff.

Takeaway: Organizations need to recognize that technology is not a substitute for the human element. Skilled cybersecurity professionals are vital for any security program. Organizations cannot spend their way out of their own workforce gap. They need to invest in their people and smartly build their teams for long-term success. For organizations that value technology investment, study participants agree that if they had enough people on staff, they would expect to increase investment in a wide array of security solutions and services they'd need to protect their organizations.

Embrace Remote Work

The global shift to remote work for many organizations has impacted cybersecurity professionals in several ways. First, they learned to work from home just like others in their organizations. Second, they had to contend with new threats and broader attack surfaces that added a new dimension to their already challenging jobs. Despite these new threats, participants cited numerous benefits of working remotely, including stronger bonds between teams, a renewed sense of mission and better communication. When asked what their organization could do to help address its own skills gap, participants cited flexible working conditions.

Takeaway: When feasible, organizations should fully embrace remote work for their cybersecurity teams. Many cybersecurity professionals want to continue working remotely, but more importantly, remote work enables organizations to cast a much wider net geographically when recruiting, which also fosters a more diverse pool of applicants.

Empower Change with DEI

Cybersecurity professionals expect their organizations to focus on DEI in order to help address their own workforce gap. Participants said they expect their organizations to invest in diversity, equity, and inclusion initiatives; encourage women and minorities to pursue STEM degrees in college; establish organizational diversity goals; and address pay and promotion gaps, if they exist. This year's study underscores that cybersecurity professionals are not only aware of how DEI initiatives can help address the talent gap, but they believe their organizations have plans to implement these programs.

Takeaway: DEI is a catalyst for positive change. Organizations that take a hard look at their own skills gap, reconsider the qualities that make a successful cybersecurity professional, focus on their people before technology and remove geographical barriers through remote work will tap into a broader pool of talent that opens up new possibilities. Cybersecurity professionals are not only aware of how DEI can contribute to solving the skills gap, but they expect their employers to act.

> **"There is way more value in working with people who think differently (even if getting along can be more of a challenge) than with people who think the same because they had the same or similar education. I have met a number of people who would be brilliant in this game but who wouldn't dream of getting into it because their backgounds are in sales, the arts, customer care, etc."**
>
> ***– Study participant***

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 membership, more than 160,000 strong, is made up of 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 2021 (ISC)² Cybersecurity Workforce Study is based on online survey data collected in collaboration with Aberdeen Strategy and Research (a Ziff Davis company) in May and June 2021 from 4,753 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.

Learn more at www.isc2.org/research.

[1] NIST Special Publication 800-181, National Institute of Standards and Technology

[2] SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president, *Reuters*, February 2021

[3] Hackers Breached Colonial Pipeline Using Compromised Password, *Bloomberg*, June 2021

[4] APAC Economic Outlook for 2021: a year of uncertainty, *IHS Markit*, January 2021

[5] Charts show that Covid is hitting parts of Asia harder now than when the pandemic began, CNBC, August 2021

[6] Asia-Pacific SMEs cautiously optimistic in the wake of COVID-19, *In The Black*, May 2021

[7] The 2021 Cybersecurity Career Pursuers Study, (ISC)²

How the Survey Was Designed

To fully understand cybersecurity needs and behaviors in the business sector, (ISC)² surveyed professionals around the world in official cybersecurity roles, as well as IT/ICT professionals who spend at least 25% of a typical work week handling cybersecurity responsibilities. These responsibilities could involve data security, security risk management/assessment, security compliance or threat detection/remediation, as well as network security architecture and monitoring, and supporting or troubleshooting cybersecurity systems. It presents a comprehensive picture of the practices, expectations and perceptions of cybersecurity professionals at all levels and stages of their careers.

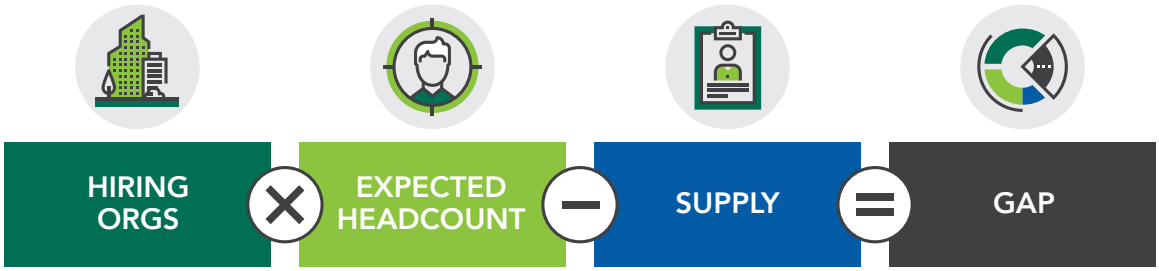
The 2021 survey includes 963 more cybersecurity professionals than 2020, continuing our goal of increasing the sample size to substantiate the validity of the results. The distribution by country, company size and other firmographics was managed closely to ensure trendability with prior waves; however, it is possible that the additional sample could have some underlying impact on the results. The margin of error for the global descriptive statistics in this research is ±1.4% at a 95% confidence level.

OUR ESTIMATION METHODOLOGY

The cybersecurity field is neither static nor simple, which means any realistic assessment demands a dynamic, holistic approach. That's why we consider several critical factors, including the percentage of organizations with open positions and an estimation of anticipated staffing needs to understand the challenges and opportunities facing both companies and cybersecurity professionals worldwide. Our supply calculation includes estimates for new entrants to the workforce (from all backgrounds) as well as professionals in other fields who are pivoting to cybersecurity.

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 globally requires reliable data from credible secondary sources (such as national census figures).

(ISC)² used a combination of methods to estimate the size of the current cybersecurity workforce:

1. **Estimate the U.S. workforce represented by cybersecurity professionals, based on population.** We estimate cybersecurity professionals' percentage of each U.S. state's labor workforce. This calculation includes the current workforce size (based on U.S. Census data) multiplied by the percentage of the expected cybersecurity workforce (based on our survey). On average, cybersecurity professionals represent 0.52% of the market's total workforce, with the U.S. range per state being 0.2% to 5.56%. For every 1 million U.S. workers, we expect to find approximately 5,200 cybersecurity professionals.

2. **Estimate the average U.S. headcount of cybersecurity professionals per business entity.** We estimate the average number of cybersecurity professionals per U.S. business entity, per state. 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 0.106 cybersecurity professionals per single U.S. business entity. For every 100,000 U.S. business establishments, we expect approximately 10,600 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. By combining and averaging figures from those three methods to reduce noise, we estimated a current U.S. workforce of 1.14M. 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 these markets' business sectors.

This estimation of the current size of the cybersecurity workforce helps ground our findings, but there are other important considerations when interpreting these estimates:

International data limitations: Accurate by-country counts of businesses outside of the U.S. are limited, and few secondary sources are available that accurately tally the total number of operating businesses globally. We use U.S. staffing ratios conservatively to extrapolate cybersecurity workforce populations outside of the U.S.; however, U.S. business dynamics and staffing models may not apply directly to international markets.

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: Since early 2020, organizations of all kinds have faced COVID-19-linked upheaval and adjustments. The survey results reflect a period of sustained uncertainty and change.