(ISC)²®

Strategies for Building and Growing Strong Cybersecurity Teams

(ISC)² CYBERSECURITY WORKFORCE STUDY, 2019

Table of Contents

Introduction

A shortage in the global cybersecurity workforce continues to be a problem for companies in all industries and of all sizes. In fact, this shortage remains the number one job concern for those working in the field. That's not surprising given that 2018 was "the year of the megabreach."[1] Municipalities are getting hit hard by ransomware,[2] and mobile malware attacks have doubled.[3]

In an era of high-profile data breaches and devastating cyberattacks, cybersecurity impacts every individual and every organization. But (ISC)² research also shows that those in the field are optimistic that those challenges can be overcome—if organizations take the right approach to growing the workforce and building strong cybersecurity teams.

For the first time, the main goal of the (ISC)² Cybersecurity Workforce Study was not only to assess the current global cybersecurity workforce gap, but also to estimate the total current number of cybersecurity professionals in the U.S. and in 10 other major global economies. Performing this workforce calculation gives organizations worldwide a better understanding of what's required for success in the cybersecurity age. By combining the workforce estimates with gap data, for example, we know that the global cybersecurity workforce needs to grow by 145% to meet the demand for skilled cybersecurity talent. In the U.S. specifically, it needs to grow 62%.

This report explores the results of the 2019 (ISC)² Cybersecurity Workforce Study, providing details on the cybersecurity workforce and gap estimates, taking a closer look at cybersecurity professionals and their teams, reviewing key steps on the cybersecurity career path, and discussing insights into immediate and longer-term methods for building qualified and resilient cybersecurity teams now and in the future.

How the Survey Was Designed

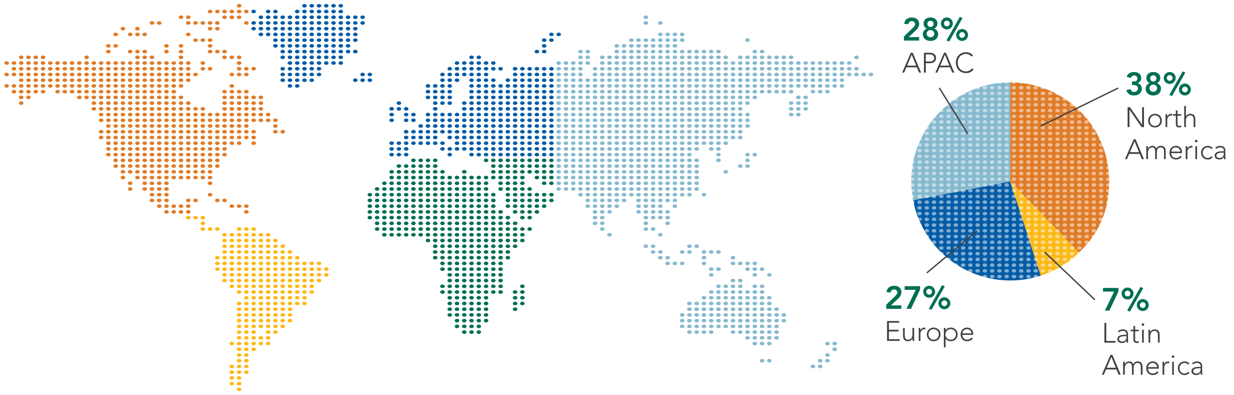
The 2019 (ISC)² Cybersecurity Workforce Study is based on online survey data collected in June and July 2019 from 3,237 individuals responsible for security/cybersecurity at work throughout North America, Europe, Latin America (LATAM) and Asia-Pacific (APAC). Respondents in non-English speaking countries completed a locally translated version of the survey. The sample 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, threat detection/remediation, 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 lower-level staff alike.

Another goal in 2019 was to expand the sample size, which in turn increases the reliability of results. We more than doubled the number of study participants from 2018 (1,452) to 3,237 in 2019. The margin of error for the global descriptive statistics in this research is plus or minus 1.7% at a 95% confidence level. See page 10 for an in-depth review of our methodology.

A LOOK AT OUR STUDY PARTICIPANTS

Geographic Distribution



Company Size Distribution

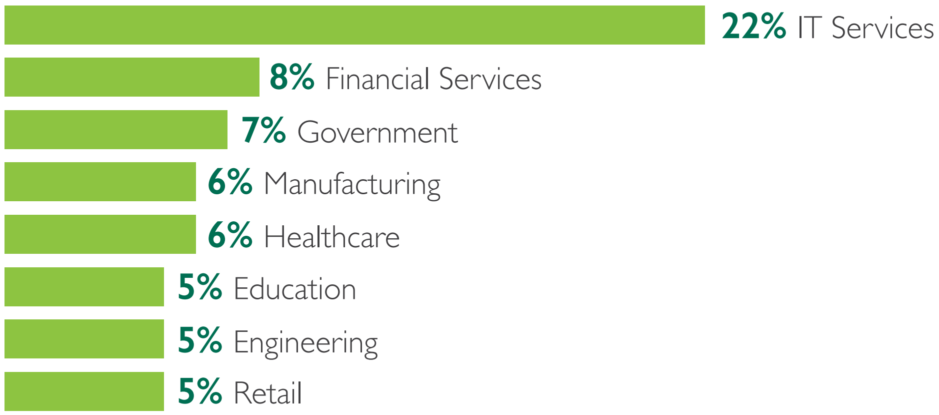
19%
1–99 employees

21%
100–499 employees

28%
500–2,499 employees

31%
2,500+ employees

Top Industry Distribution



The Cybersecurity Workforce Estimate

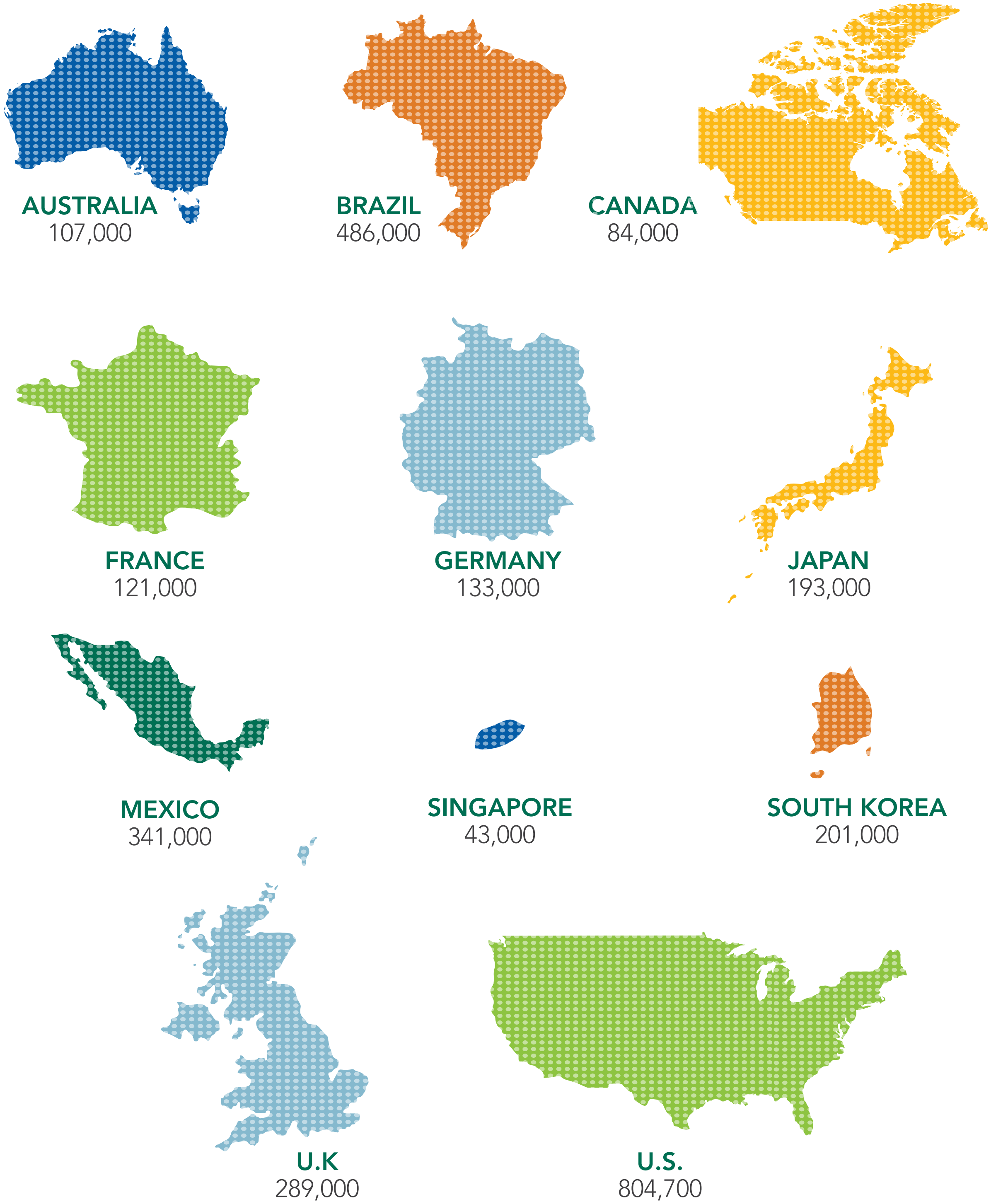
Our goal with the 2019 (ISC)² Cybersecurity Workforce Study was to go beyond traditional gap calculations and relate the results back to the broader business ecosystem. To accomplish this goal, we developed a method to estimate the size of the current cybersecurity workforce, a measurement not currently provided by publicly available sources.

This calculation process was finalized first for the U.S., based on the availability of the most robust market inputs. The study found that nearly 805,000 cybersecurity professionals are estimated to be working in the U.S. The calculation was then applied to 10 other major economies where sufficient survey data was available. Together, these workforce estimates total 2.8 million.

Our calculation 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 necessarily apply directly to international markets.

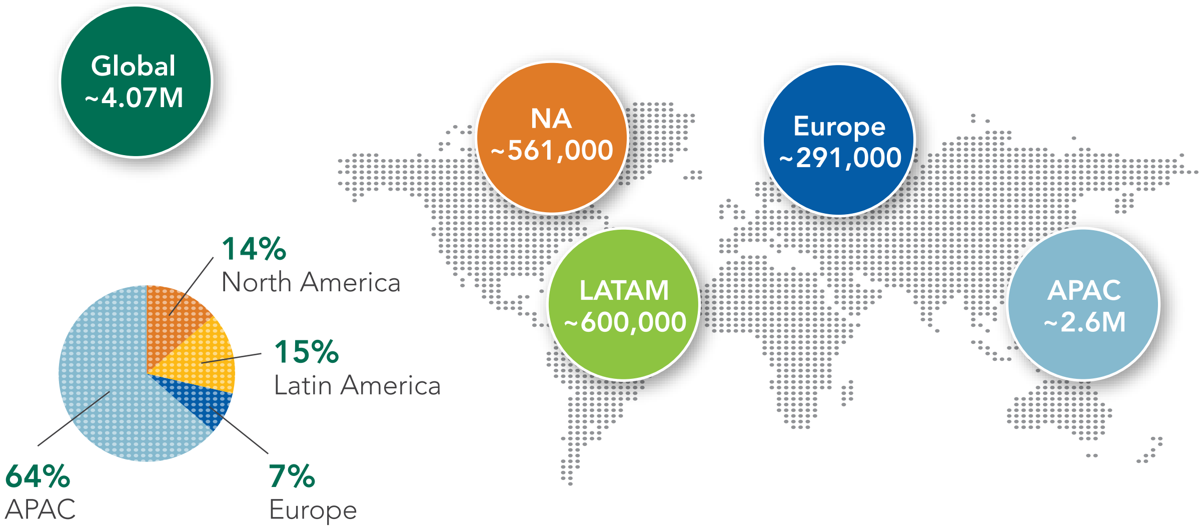
As a result, the size of current global cybersecurity workforce should be considered our best estimate, given the lack of secondary data sources available in some regions.

GLOBAL CYBERSECURITY WORKFORCE ESTIMATES



The Cybersecurity Workforce Study shows that these cybersecurity and IT professionals are generally satisfied in their careers and optimistic about their futures. But the size of the current workforce still leaves a significant gap between the number of cybersecurity professionals working in the field and the number needed to keep organizations safe.

The Cybersecurity Workforce Gap by Region



The cybersecurity workforce gap has increased since last year, primarily due to a global surge in hiring demand. In the U.S., the cybersecurity workforce gap is nearly 500,000. By combining our U.S. cybersecurity workforce estimates and this gap data, we can calculate that the cybersecurity workforce needs to grow by 62% in order to meet the demands of U.S. businesses today. Using the workforce estimate of 2.8 million based on the 11 economies for which we provided a workforce estimate and the global gap estimate of 4.07 million, we can estimate that the global workforce needs to grow by 145%. It's a big task, but our intent is to provide a goal for growing the workforce to help meet increasing demand for cybersecurity professionals.

In Europe, where the gap has almost doubled, we see an increasing hiring demand emerging in smaller companies with 1 to 99 employees and in companies with 500+ employees. In LATAM, where the gap has increased more significantly, we see stronger demand emerging in midsized companies with 100 to 499 employees as well as in large companies. The good news is that, despite increased hiring demand, the gap widened very little for North America and for APAC.

In this year's study, 65% of organizations represented have a shortage of staff dedicated to cybersecurity. That lack of skilled/experienced cybersecurity personnel is the top concern among survey respondents—even more of a concern than a lack of resources to do their jobs effectively. In addition, 51% of cybersecurity professionals say their organization is at moderate or extreme risk due to cybersecurity staff shortage.

Top Job Concerns Among Cybersecurity Professionals

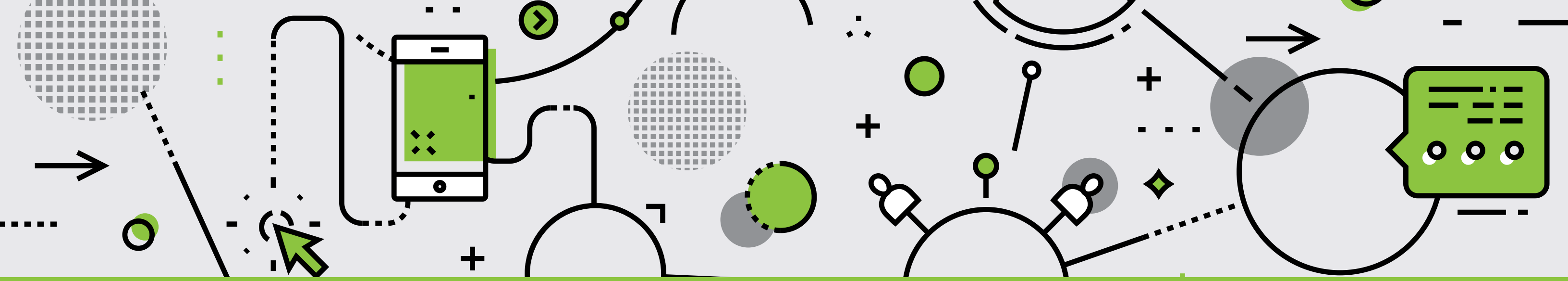
36%
Lack of skilled/experienced cybersecurity security personnel

28%
Lack of standard terminology for effective communication

27%
Lack of resources to do my job effectively

24%
Lack of work-life balance

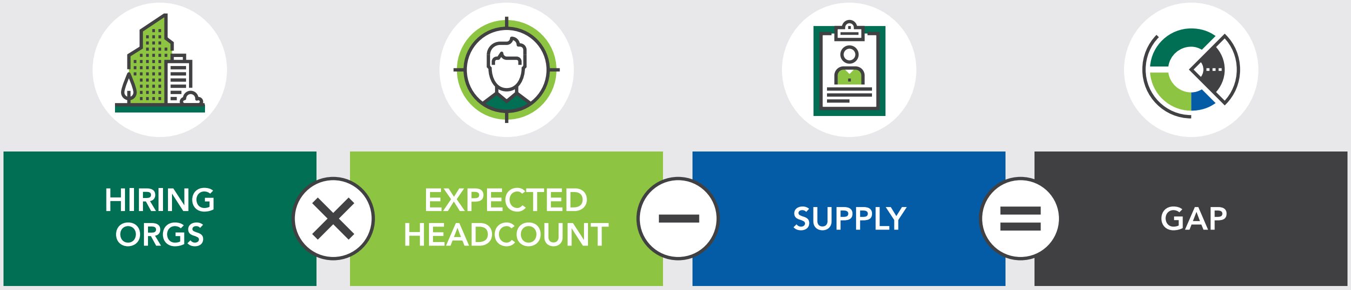
24%
Inadequate budget for key security initiatives



OUR ESTIMATION METHODOLOGY

Unlike legacy gap calculation models that simply subtract supply from demand, our calculation takes other critical factors into consideration, including the percentage of organizations with open positions and the estimated growth of companies of different sizes. The calculation of demand includes the openings that are currently available, along with an estimation of future staffing needs. The calculation of supply includes estimates for academic and non-academic entrants into the field, along with estimates of existing professionals who are pivoting to cybersecurity specialties. This more holistic approach to measuring the gap produces a more realistic representation of the security challenges—and opportunities—that both companies and cybersecurity professionals are facing worldwide.

Gap Calculation



HIRING ORGS × EXPECTED HEADCOUNT − SUPPLY = GAP

The Cybersecurity Workforce Study provides us with robust cybersecurity headcount volume across all company sizes, but only among survey respondents. To extrapolate the cybersecurity headcount volume by country, data for the total count of operational businesses, by number of employees, is necessary from credible secondary sources (e.g., national census).

With these inputs, there are several ways to calculate the workforce projection, and (ISC)² used a combination of three methods to derive the current size of the cybersecurity workforce:

1. **Estimate of U.S. workforce represented by cybersecurity professionals.** This is a population-based average. Per U.S. state, we estimate the percentage of labor workforce cybersecurity professionals represented. This calculation includes the current workforce size (based on U.S. Census data) multiplied by the percent of the expected cybersecurity workforce (based on the survey). On average, cybersecurity professionals represent 0.43% of the market's total workforce, with the U.S. range per state being 0.16% to 3.81%. For every 1 million U.S. workers, we'd expect 4,300 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 0.10 cybersecurity professionals per single U.S. business entity. For every 100,000 U.S. business establishments, we expect 10,000 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 U.S. calculation. The total U.S. business establishments and company size share distribution (from U.S. Census data) was multiplied by the expected cybersecurity headcount per establishment (from the survey). Focusing only on survey inputs, we determined the ratios of average cybersecurity professionals by company size. For all U.S. business establishments, we expect 901,700 to 1.05 million total cybersecurity professionals.

Results from all three calculation methods were statistically pooled to help moderate potential noise from any single calculation. By combining and averaging figures from those three methods, we're able to estimate a current workforce of 804,700 individuals in the U.S.

After finalizing the calculation process for the U.S., given the availability of the most robust market inputs, we then applied it to 10 other countries where sufficient survey data was available: Canada, Mexico, Brazil, the U.K., France, Germany, 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 these nations have extremely large populations, and have been experiencing rapid economic growth, adding China and India into our cybersecurity workforce estimation would introduce the potential to exponentially overstate the actual number of cybersecurity professionals.

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

International limitation: 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 determine the total number of operating businesses internationally. Again, our estimate uses U.S. staffing ratios conservatively to extrapolate cybersecurity workforce populations outside of the U.S.; however, we certainly recognize that U.S. business dynamics and staffing models may not necessarily apply directly to international markets. As a result, the size of the current global cybersecurity workforce should be considered our best estimate, given the lack of secondary data sources available in some regions.

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

What Today's Cybersecurity Workforce Looks Like

The professionals tasked with protecting their organization's critical assets go by many titles: IT security director or manager, security architect/engineer, security specialist, consultant, advisor, or simply IT staff.

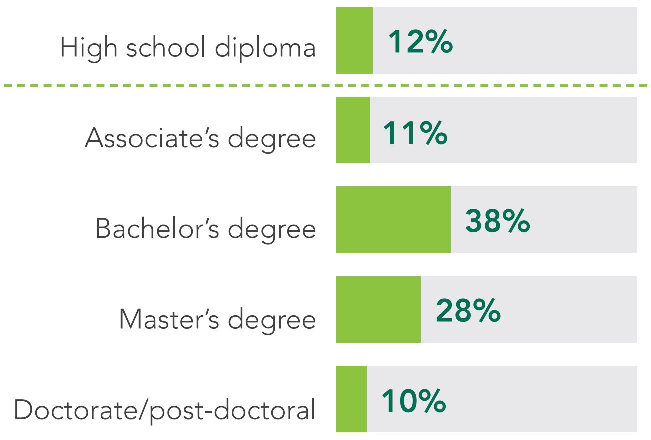
The Titles They Hold

- Exec/CXO
- CISO
- IT Director
- IT Security Director
- IT Manager
- IT Security Manager
- Security Architect/Engineer
- Security Specialist
- Security Consultant/Advisor
- Security Analyst
- Security/Compliance Officer
- Security Administrator
- IT Staff
- Application Developer/Tester

Cybersecurity professionals are likely to have at least a bachelor's degree—with a little more than one-third holding a master's or doctoral/post-doctoral degree. While most in the field get their degrees in computer and information sciences (40%), others get degrees that are not IT-focused, such as engineering (19%) and business (10%).

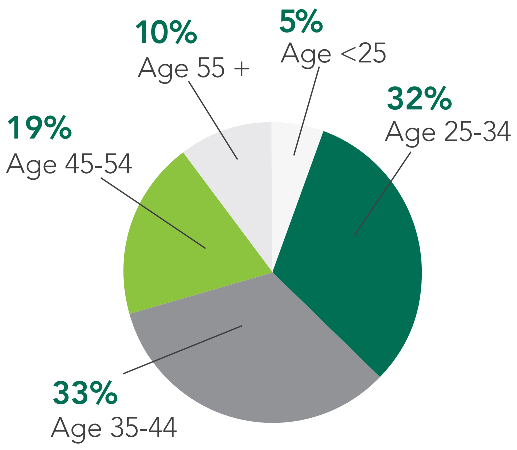
What Do Cybersecurity Professionals Look Like?

EDUCATION



Computer and information sciences: **40%**
Engineering: **19%**
Business: **10%**

AGE



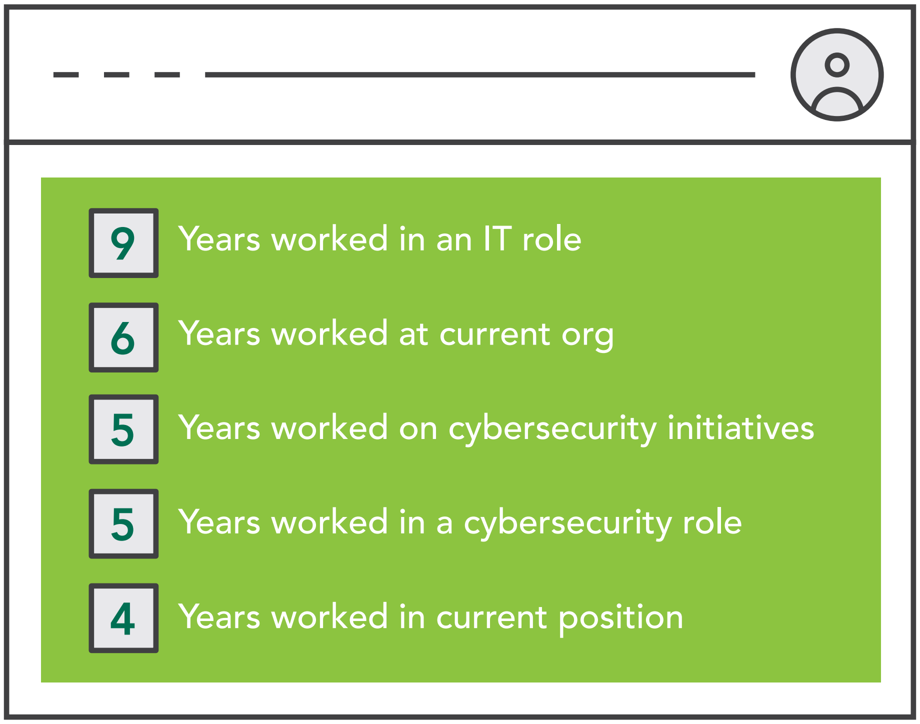
> **"We must never stop learning our trade craft—there is always more to learn in order to stay ahead of the bad actors."**
>
> ***– Study participant***

A Closer Look at Cybersecurity Professionals

Cybersecurity professionals are more than twice as likely to be male, meaning there is an under-tapped demographic available for recruiting if companies can position the role in a way that overcomes common stereotypes. 30% of survey respondents were women. Among respondents with security-specific titles, 23% of study participants were women. The highest percentage of women cybersecurity professionals came from LATAM (39%) and North America (34%).

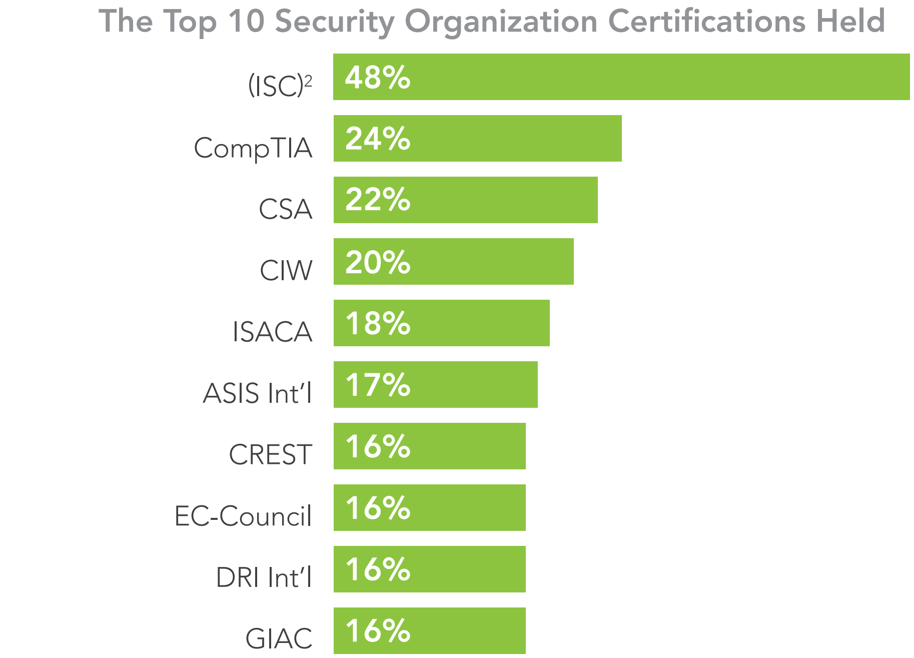
Cybersecurity professionals tend to be experienced and long-tenured where they work: Survey respondents have an average of nine years in an IT role, with six years at their current organization and five years in a cybersecurity role. On average, they hold about four security organization certifications and three security organization memberships.

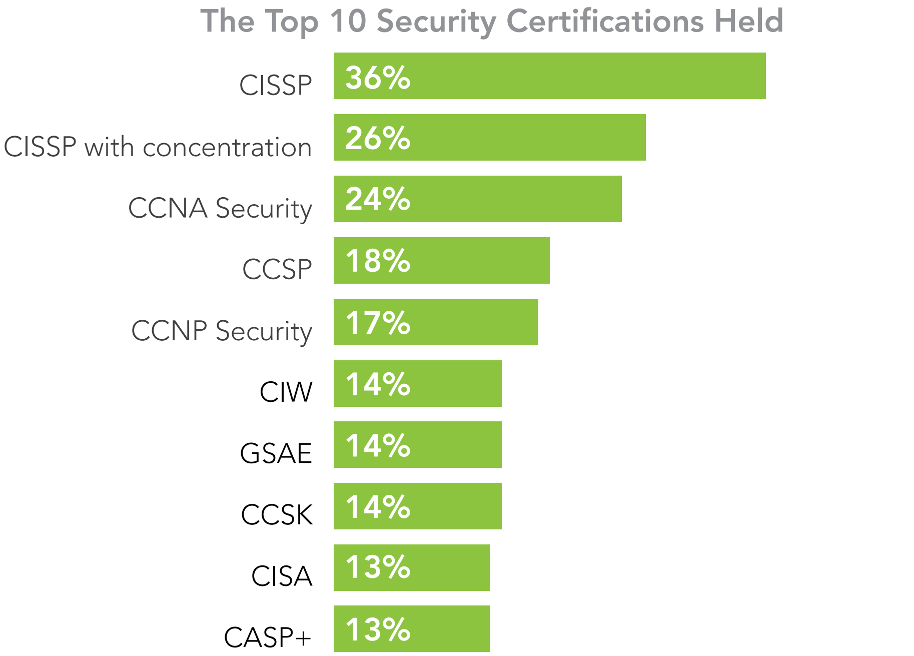
A Cybersecurity Resume



9	Years worked in an IT role
6	Years worked at current org
5	Years worked on cybersecurity initiatives
5	Years worked in a cybersecurity role
4	Years worked in current position

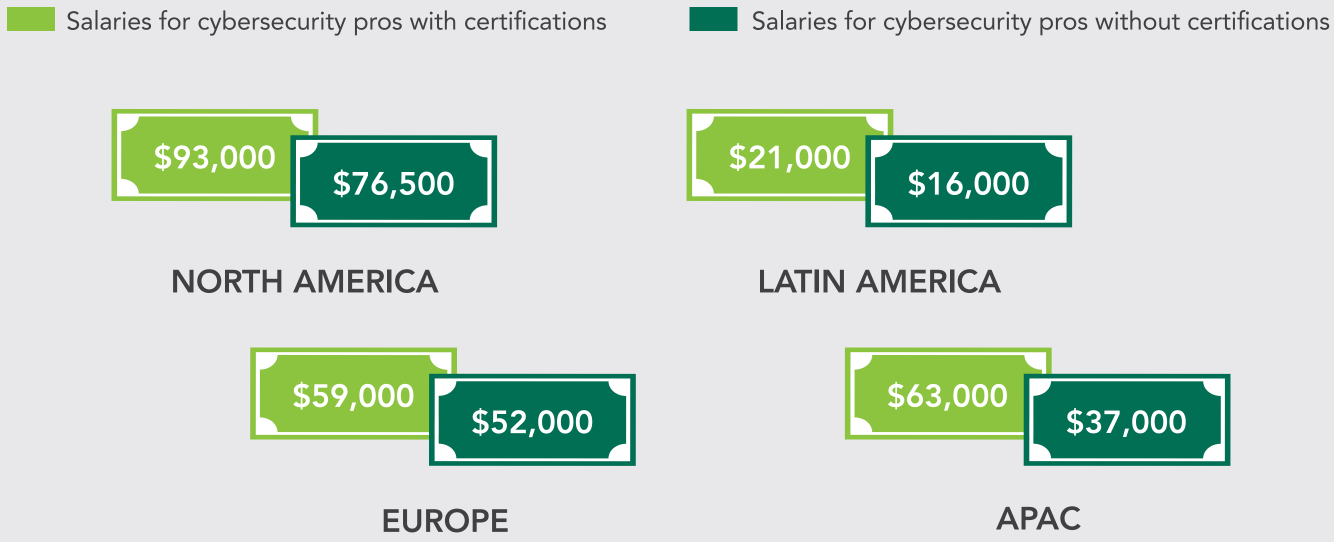
Security Certifications Held by Cybersecurity Professionals





Cybersecurity professionals make about U.S. $69,000 per year, on average. The average salary is highest in North America ($90,000) and lowest in LATAM ($20,000), with APAC ($59,000) and Europe ($58,000) falling in between. Those holding security certifications have an average salary of $71,000 while those without earn much less—about $55,000, on average.

The Impact of Certifications on Salaries



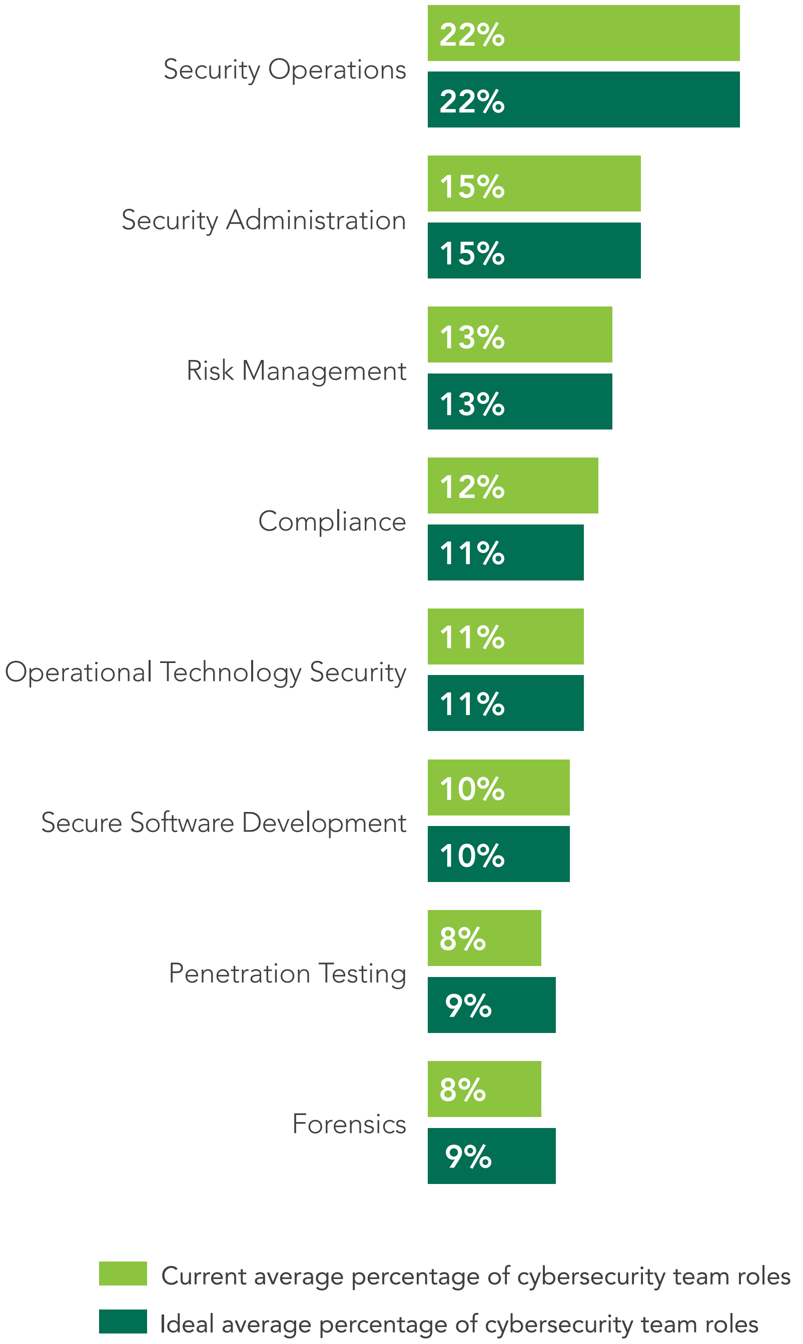
A Closer Look at Cybersecurity Roles

Cybersecurity initiatives at the majority of the represented organizations are led by a chief information security officer (CISO). That's particularly common in organizations with 500 or more employees. Among those organizations, 62% are led by a CISO, with 27% being led by a senior IT executive. Among smaller organizations, the split is closer to 50% led by a CISO and 30% led by a senior IT executive.

> **"Cybersecurity is all about people, not just the processes and technology."**
>
> ***– Study participant***

Organizations are distributing key roles and responsibilities across their cybersecurity teams in a way that closely aligns with respondents' ideal team structures.

Cybersecurity Team Roles



Slightly more emphasis is being placed on roles like security operations, security administration, risk management and compliance, with cybersecurity teams allocating 63% of their resources to these roles, on average. Specialized cybersecurity roles like operational technology security, secure software development, penetration testing and forensics account for about 37% of cybersecurity team resources, on average.

Cybersecurity teams in North America allocate slightly more team resources on security operations, security administration and compliance roles than any other region. Forensics roles are slightly more prevalent on cybersecurity teams in Europe. And while compliance roles are less prevalent for LATAM and APAC cybersecurity teams, more focus is placed on roles like operational technology security and secure software development.

Average Number of Employees in Each Role (Across All Company Sizes)

Cybersecurity team roles	Total	NA	LATAM	EUR	APAC
Security Operations	22	23	19	22	22
Security Administration	15	16	15	15	15
Risk Management	13	13	13	13	13
Compliance	12	13	10	12	11
Operational Technology Security	11	11	14	11	12
Secure Software Development	10	9	12	9	11
Penetration Testing	8	8	9	9	9
Forensics	8	8	8	9	8

The distribution of roles varies slightly by company size as well. Small companies with 1 to 99 employees are staffing their cybersecurity teams with more general roles like security operations and security administration than are larger organizations. Midsized companies with 100 to 499 employees are allocating a slightly higher proportion of team resources to handling risk management and compliance responsibilities. And large companies with 500+ employees are more likely to have more specialized roles like secure software development, penetration testing and forensics on their cybersecurity teams than are smaller companies.

Average Number of Employees in Each Role (by Company Size)

Cybersecurity team roles	Total	1–99	100–499	500+
Security Operations	22	23	21	22
Security Administration	15	17	16	15
Risk Management	13	13	14	13
Compliance	12	12	13	12
Operational Technology Security	11	11	11	11
Secure Software Development	10	9	9	10
Penetration Testing	8	8	8	9
Forensics	8	7	8	8

The tables below show by company size the roles where organizations may be overstaffed (green up arrows) and the roles where organizations may be understaffed (red down arrows).

Small organizations are currently doing a solid job at staffing and distributing roles on their cybersecurity teams. They could potentially look to reduce or reallocate risk management roles/resources to other areas that may need focus. Midsized organizations are also doing a good job staffing roles on their cybersecurity teams but could potentially create more security operations and operational technology security roles on their teams.

While large companies may have the most resources in terms of staffing, they may need to take a closer look at how those resources are currently allocated across roles on their cybersecurity teams. Roles that may be currently understaffed include security operations, security administration, risk management and penetration testing. Roles that may be currently overstaffed include compliance, forensics and operational technology security.

Cybersecurity team roles by company size (condensed)	1–99	100–499	500 +
Security Operations	–	▼	▼
Security Administration	–	–	▼
Risk Management	▲	▲	▼
Compliance	–	–	▲
Forensics	–	–	▲
Penetration Testing	–	–	▼
Secure Software Development	–	–	–
Operational Technology Security	–	▼	▲

Cybersecurity team roles by company size (expanded)	1–19	20–49	50–99	100–249	250–499	500–999	1,000–2,499	2,500–4,999	5,000–9,999	10,000 +
Security Operations	–	–	–	–	▼	▼	–	–	▲	▼
Security Administration	–	–	–	–	–	▲	–	–	▼	–
Risk Management	▲	–	–	–	▲	–	–	▼	▲	–
Compliance	–	–	–	–	–	–	▲	▲	–	▲
Forensics	–	–	–	–	–	–	–	–	–	▲
Penetration Testing	–	–	–	–	–	–	▼	–	▼	–
Secure Software Development	–	–	–	–	–	–	–	▼	▲	–
Operational Technology Security	–	–	–	–	▼	–	▲	–	▲	–

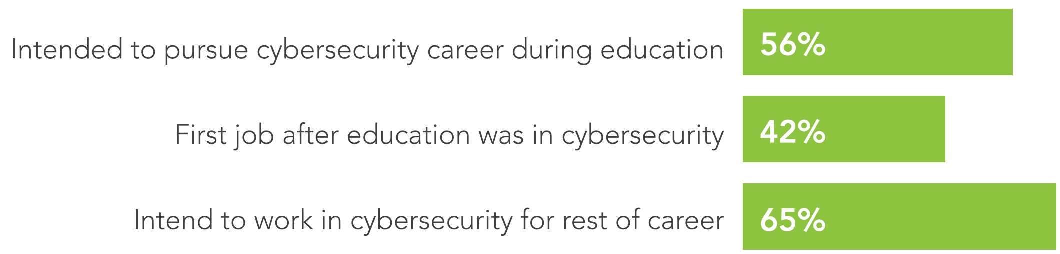
The Cybersecurity Career Path

While most of those in cybersecurity (56%) intended to work in this field—and most plan to remain in it for the rest of their careers—few started in it: Just 42% of respondents' first jobs after education were in cybersecurity.

That desire for a cybersecurity career revolved around the high demand for cybersecurity skills and the rapidly changing challenges that keep the job interesting. These prospects-turned-professionals also saw that the growing field offered job security and was continuously evolving while allowing them to put their skills to use in nearly every industry.

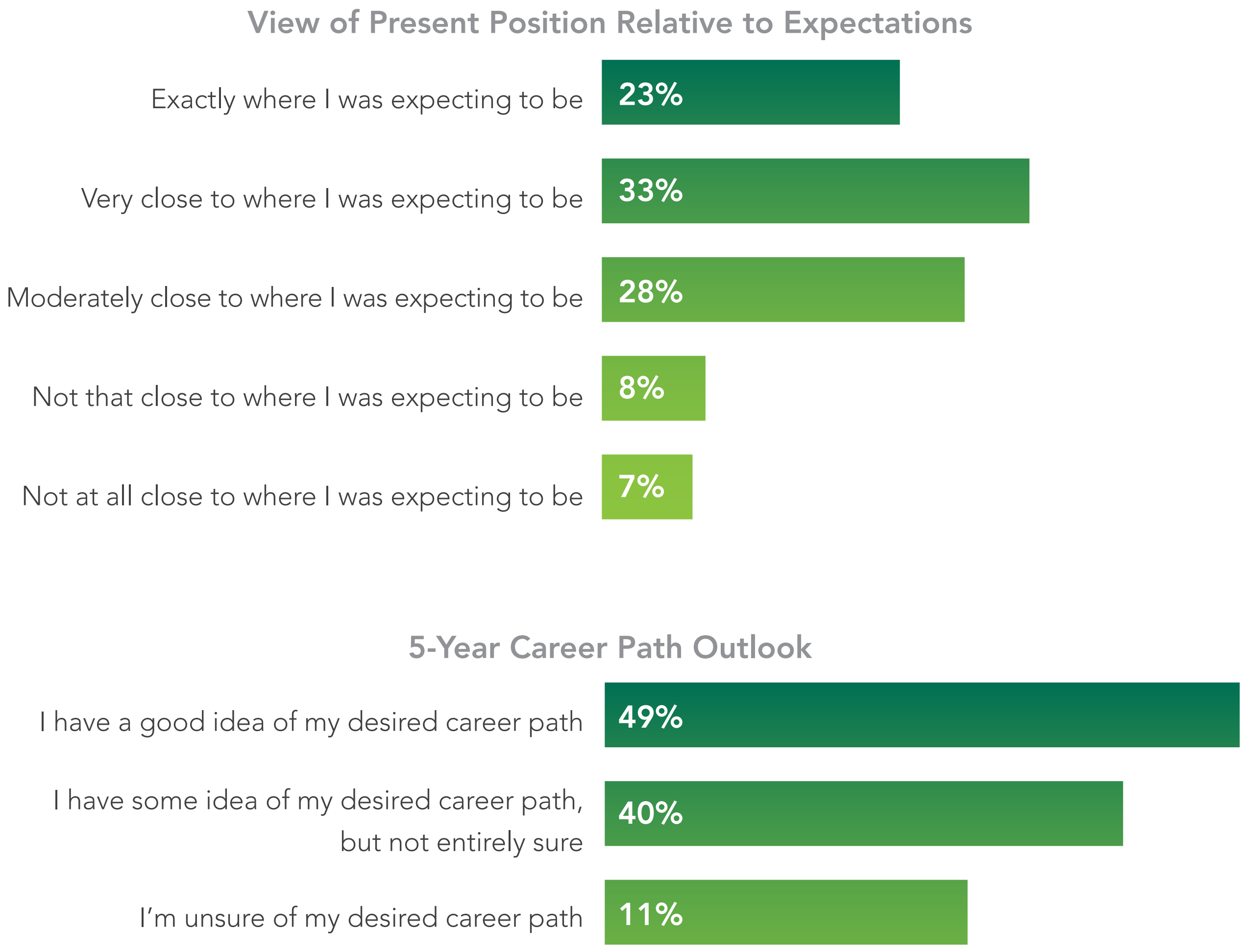
They're motivated to continue their careers for the same reasons: the high demand, the ability to work in a continuously evolving field, the ability to constantly solve puzzles and never get bored, and job security. A strong majority—65%—intend to work in cybersecurity for the rest of their careers.

Getting Started in Cybersecurity



Helping to drive job satisfaction is that the demand for cybersecurity skills creates a predictable career path that's still intriguing. The vast majority of respondents (84%) say they are where they expected to be in their careers, given their skills and experience. Well over half say they are either very close or *exactly* where they expected to be. Almost half also say they have a good idea of their desired career path looking forward.

Cybersecurity Career Check-in



Respondents noted numerous successes they have experienced as a cybersecurity professional, from becoming the go-to source of information for their colleagues to taking the lead on major security projects. They've raised their profile within the company, served as mentors to other employees and been assigned to leadership positions.

Relevant experience is the key to that success, the study shows. Other keys include:

Robust training and professional development

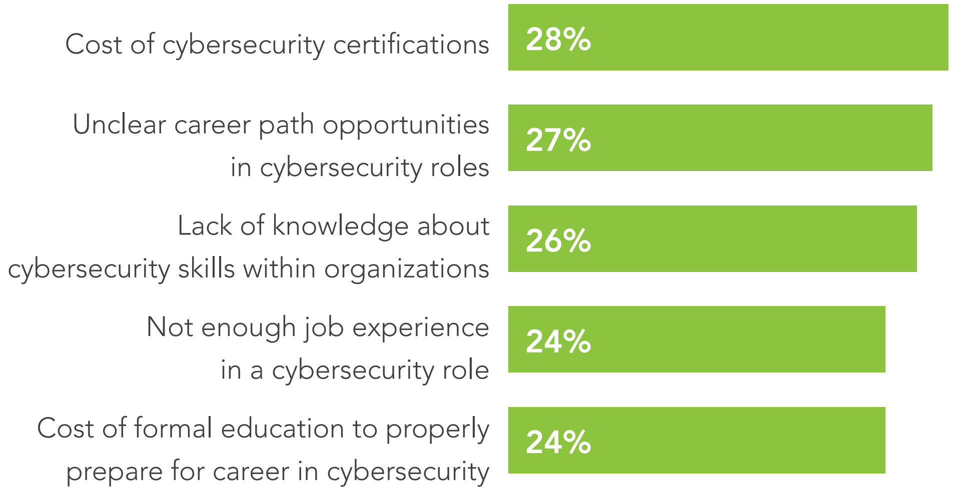
Working for companies with innovative cybersecurity tools and technology

Supportive management

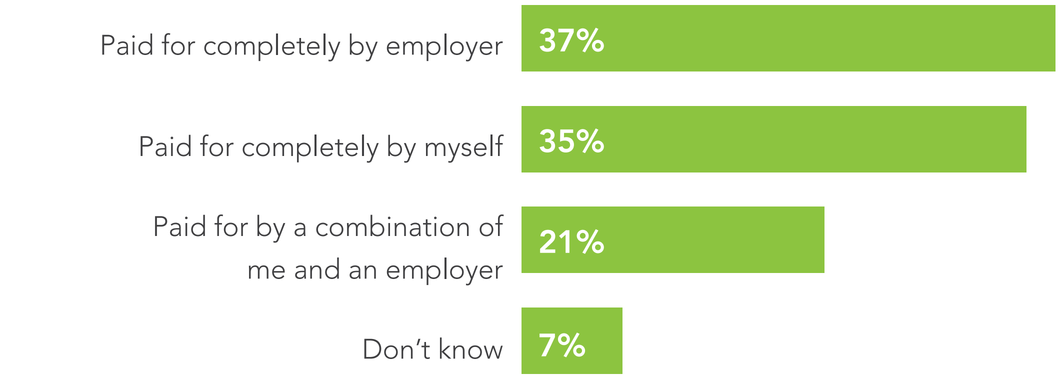
Strong professional mentorship

But as with any job, there are career stumbling blocks, which organizations can help cybersecurity professionals overcome. The cost of cybersecurity certification is the number one career hurdle, with more than half of respondents having to pay out-of-pocket for at least some of the costs of cybersecurity certifications.

Key Items Hindering Career Progression



Who Pays for Cybersecurity Certificates?

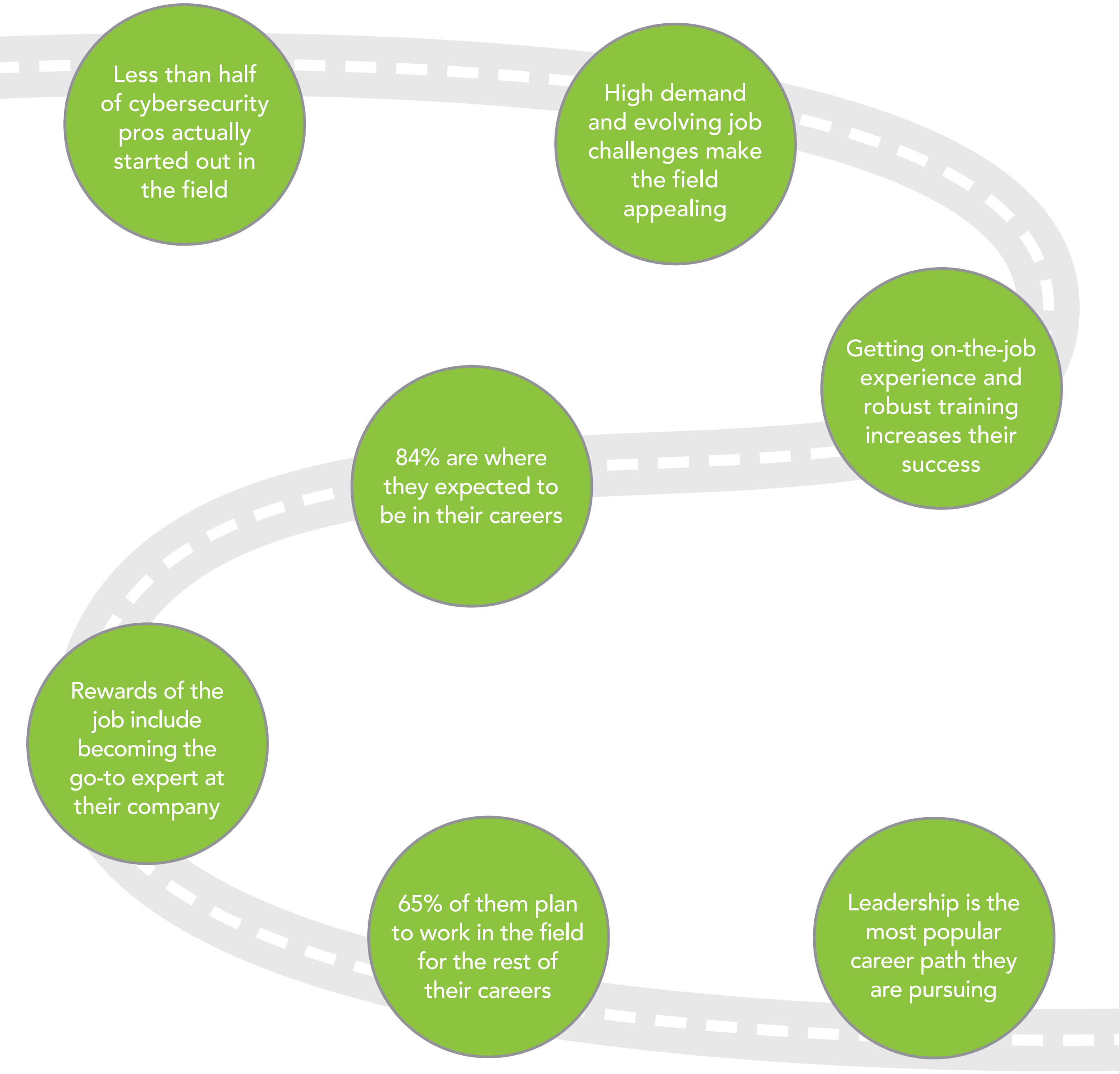


By picking up that cost, organizations can help keep their cybersecurity professionals satisfied and more fulfilled, increasing the possibility that these professionals will remain at their current organization while increasing the vital knowledge of their cybersecurity teams.

Respondents whose organizations pick up that tab display significantly higher job satisfaction rates than their peers who aren't as fortunate. 72% of those respondents 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.

> **"We're trying to help everyone protect themselves, and becoming a great cybersecurity professional takes time, patience, dedication, and support from the top."**
>
> ***– Study participant***

Progressing Along the Cybersecurity Career Path



Less than half of cybersecurity pros actually started out in the field

High demand and evolving job challenges make the field appealing

Getting on-the-job experience and robust training increases their success

84% are where they expected to be in their careers

Rewards of the job include becoming the go-to expert at their company

65% of them plan to work in the field for the rest of their careers

Leadership is the most popular career path they are pursuing

Building Cyber-Strong Teams

Growing a strong cybersecurity workforce with the appropriate staffing levels is challenging but not impossible to achieve, especially when you put these two methods to use:

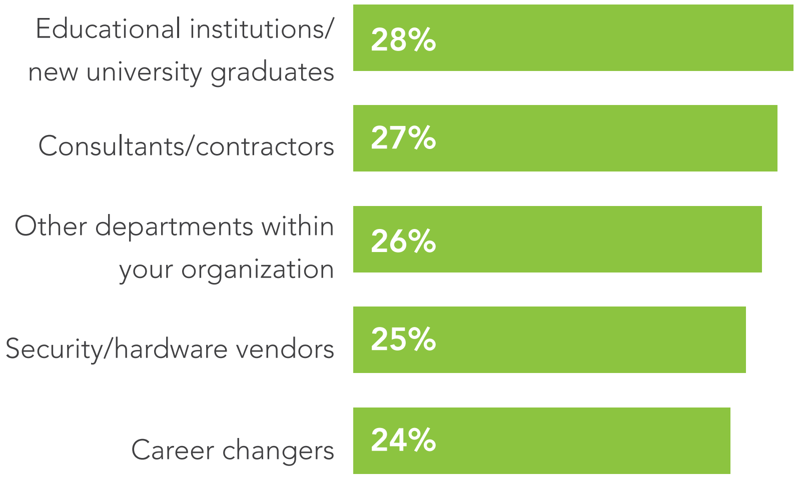
- In the near term, recruiting new workers from multiple sources to grow the team from the outside in
- In the longer term, further developing existing IT professionals as cybersecurity experts to grow the team from the inside

Building Teams from the Outside in

The most direct near-term solution for building a strong team is to recruit and hire new professionals. That's the approach half of the represented organizations plan to take over the next year. But in a tight job market, where are they finding these recruits?

New graduates and people looking to change careers are two primary sources. But organizations respect the knowledge that comes from experience, too. They're looking for relevant and extensive work experience, advanced knowledge of concepts, and cybersecurity certifications. So they're also seeking to hire people who are currently acting as consultants, contractors, and working within security and hardware vendors.

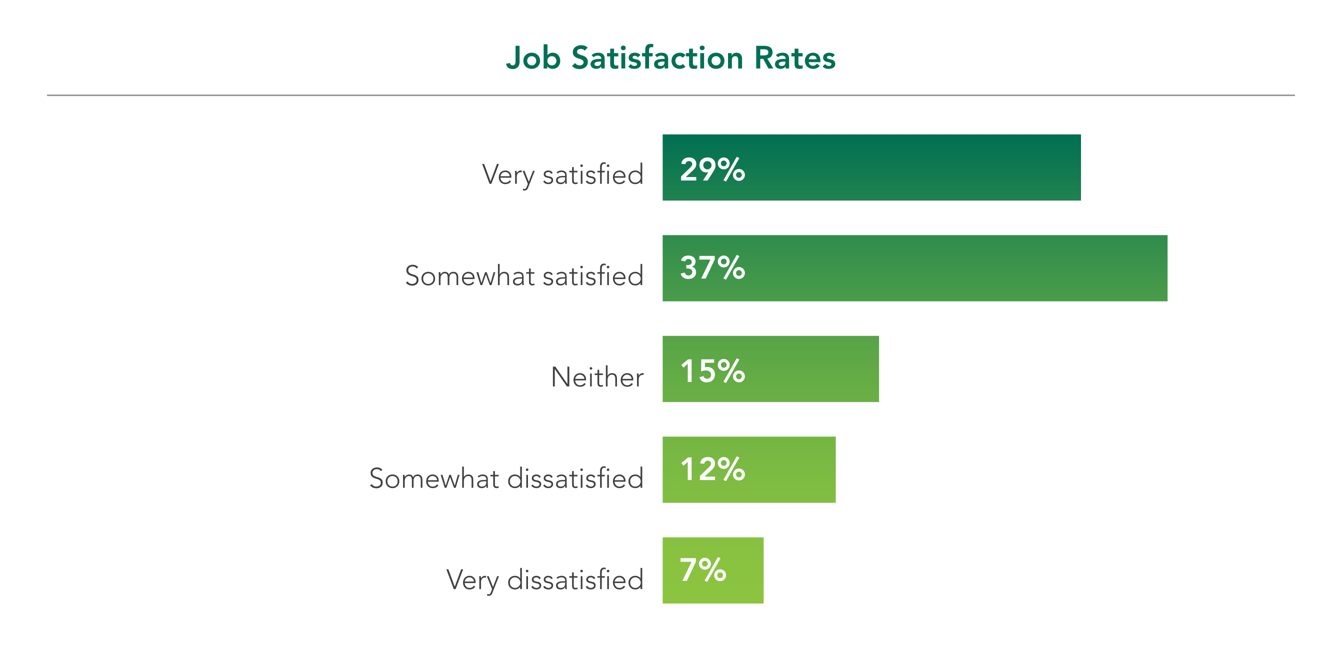
Top Recruiting Sources



Organizations in LATAM and APAC are more likely than others to recruit from educational institutions and security/hardware vendors. Organizations in North America and Europe are more likely than others to recruit consultants.

> **"Some of the most talented information security professionals I've met did not come from the traditional IT background, but from other sectors. Information security is a great career-change option."**
>
> ***– Study participant***

Clear descriptions of job roles and responsibilities should aid in recruiting. Cybersecurity is an attractive job for those just getting into the field as well as for those who have been doing it for any length of time, according to the study. Job satisfaction is high, especially in the North America, where 71% of respondents say they are satisfied with their jobs and 36% say they are very satisfied. Respondents in APAC reported the lowest satisfaction rates, with 62% saying they are satisfied with their jobs and only 21% saying they are very satisfied.



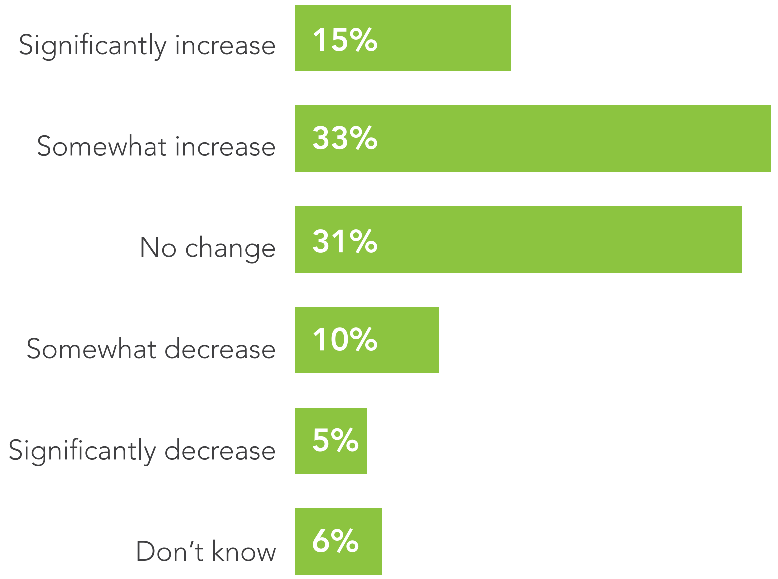
Knowing that job satisfaction is high among cybersecurity professionals should provide organizations with added confidence to make job descriptions and responsibilities as accurate as possible. This ensures there are no surprises for new hires, and it will assist in attracting and identifying the best candidates.

Building Teams from the Inside

Another method for building a strong team is to draw on employees from within the organization. And because experience is important, many organizations intend to keep their in-house experts in place and help them further develop the constantly evolving skills and knowledge needed to secure their organizations in the future. In building their cybersecurity teams, 70% of organizations give priority to training and promoting from within, according to previous (ISC)² research. 57% offer training and certification opportunities to employees to strengthen their teams, and 55% offer cross-training on cybersecurity skills and responsibilities.[4]

Almost half of organizations represented in the Cybersecurity Workforce Study are planning to increase their security training budgets within the next year. That's a good thing, because the vast majority of study participants (81%) say they need additional certifications or training to prepare for future roles.

Changes to Security Training Budgets in the Next Year

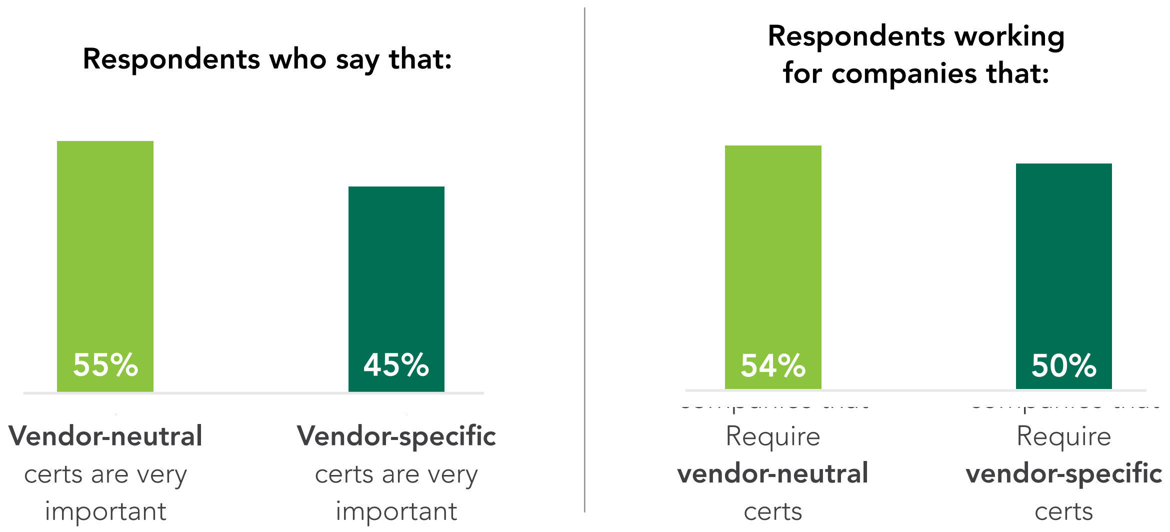


Respondents indicated a number of specific areas where they feel the need to further develop or improve their skills

- Cloud computing security
- Risk assessment, analysis, and management
- Governance, risk management and compliance (GRC)
- Security and threat intelligence analysis
- Security engineering and administration
- Penetration testing
- Intrusion detection
- Network monitoring

When it comes to certifications, 55% of respondents feel that vendor-neutral certifications are very important, and 54% report that vendor-neutral certifications are required in their organizations. While less important in comparison, vendor-specific certifications are still seen as very important by 45% of respondents and are required by half of their organizations. The vast majority of respondents—81%—anticipate that they will need to obtain additional certifications or training as they prepare for future roles.

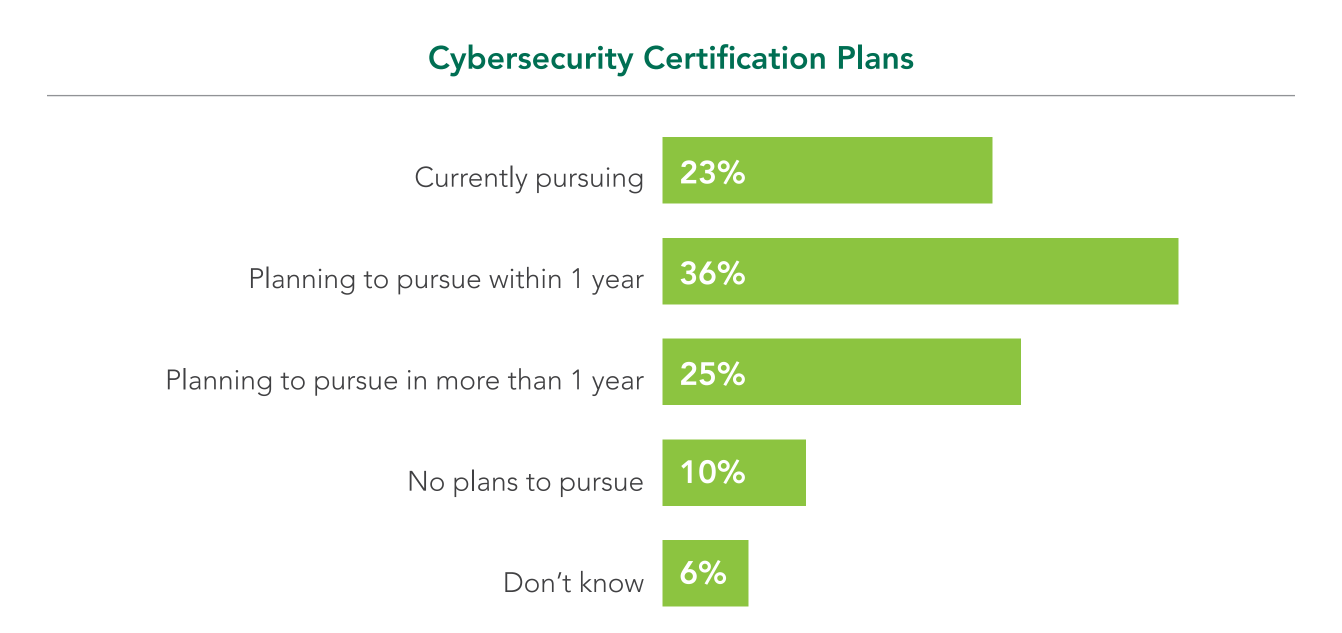
The Value of Certifications



Respondents who say that:

Respondents working for companies that:

As a result, 84% of cybersecurity professionals are planning to pursue a new cybersecurity certification at some point. 59% are currently pursuing a new cyber certification or plan to do so within the next year.



Their motivations for getting those certifications revolve mostly around a desire to improve in their job or to learn more. In fact, according to respondents, the top motivator for getting a cybersecurity certification is to improve or add to a skill set. Other motivators include staying competitive in the industry, advancing their career and becoming an expert. Much farther down the list is the desire to make more money.

> **"To be an effective cybersecurity professional, you have to have a broad, detailed understanding of all components of IT, and those with cybersecurity certifications have skills far beyond what is required of other certifications."**
>
> ***– Study participant***

Motivations for Pursuing Certifications

40%
To improve/add to skill set

39%
To stay competitive

38%
To learn more

38%
To advance/develop career

33%
To become an expert

29%
To make more money

28%
To earn associated certification or credential to put on a resume

27%
To change or explore a new cybersecurity career path

By helping their in-house IT professionals—those currently on staff and new hires—develop their cybersecurity skills and stay abreast of the newest innovations through training and certifications, organizations can take a significant step toward building a strong cyber-resilient team.

Developing Your Cybersecurity Dream Team

Key to growing a strong cybersecurity workforce is making sure your organization offers both an appealing team to join and a rewarding place to stay.

STRATEGY #1 is to make sure your organization appeals to cybersecurity professionals by addressing their most important needs. Start by highlighting the opportunities that contribute most to a successful cybersecurity career, including relevant on-the-job work experience, robust training and professional development and access to career advancement opportunities.

Offer opportunities to nurture and develop the areas that are top of mind for cybersecurity professionals, such as:

- Cloud computing security
- Risk assessment, analysis and management
- Governance, risk management and compliance (GRC)
- Security and threat intelligence analysis

You can also help mitigate the typical challenges cybersecurity professionals face in their career progression by:

- Contributing toward the cost of cybersecurity certifications
- Laying out a clear career path toward specific cybersecurity roles
- Educating the organization on what cybersecurity means for the organization, what kind of skills it requires, and what roles these professionals serve
- Providing the opportunity to keep up to date on cybersecurity trends
- Providing the opportunity to increase security awareness among end users

Finally, you can appeal to the motivations that both initially enticed and continue to motivate cybersecurity professionals in their careers. Focus on the opportunity to work in a continuously evolving field that offers job stability and security as well as a challenging work environment full of puzzles that need solving, ensuring that they'll never get bored.

STRATEGY #2 is to level-set on cybersecurity applicant qualifications based on what a cybersecurity professional's background really looks like. When it comes to education, they may have a Bachelor's degree, but 11% of your potential recruits globally have only a two-year degree, and 12% have only a high school diploma. And while most come from a computer and information sciences background, over a quarter (29%) will come with backgrounds in business or engineering instead.

Given that the majority of cybersecurity professionals wear many hats and have IT responsibilities beyond cybersecurity, 70% of qualified cybersecurity recruits will have a title that isn't specific to security.

As for salary, align your expectations appropriately to account for factors like your organization's size and the certifications your applicant has. Cybersecurity professionals at larger organizations tend to make 18.6% more than those at smaller organizations, and those with certifications are earning higher salaries than those without.

Also, be realistic about requirements for certifications based on the level of position you are hiring. Many entry-level and even mid-level positions will be appealing to candidates without the years of experience required to earn many of today's in-demand cybersecurity certifications. But as our study has revealed, these professionals will be driven to obtain those certifications during their career, which will provide you with even more confidence in your cybersecurity team.

STRATEGY #3 is to grow your cybersecurity workforce by recruiting new workers to join your organization. Start by going after new workforce entrants such as recent college graduates who have degrees that are relevant to starting a cybersecurity career, including computer and information sciences and engineering. Highlight the aforementioned benefits of the cybersecurity field.

Then, look for more seasoned professionals who may have previous cybersecurity work experience and knowledge of advanced cybersecurity concepts. Organizations are considering consultants and contractors, employees of security and hardware vendors, employees from other companies within their industries, and employees at managed security services providers (MSSPs). But it may make more sense for you to augment your staff with an MSSP's services.

Don't underestimate the power of certifications when it comes to job satisfaction and recruiting. The majority of cybersecurity professionals feel that certifications are critical to their success, and those working for organizations that pay for their certifications are significantly more satisfied in their role (72%) than those working for organizations that don't (63%). Offer certifications and training in the areas that cybersecurity professionals are most interested in, including the ones listed above.

STRATEGY #4 is to grow your cybersecurity workforce from within by further developing your existing IT pros. Start by identifying talented and motivated non-security-focused IT professionals and paying for cybersecurity trainings and/or certifications. IT generalists have a solid foundation to contribute to an organization's cybersecurity practice. But more importantly, for many organizations, cybersecurity is a joint responsibility, and developing IT pros to be more effective cybersecurity practitioners benefits the entire organization.

You can also find talented internal employees with transferable skills in other departments, such as legal, finance, HR and even marketing. Look for employees with a clear understanding of how data flows through your organization, or those experienced in legal and compliance controls or user training, then determine their interest in developing skills to become a cybersecurity professional. Remember that paying for certifications and training can be an incentive to make the transition and can promote higher job satisfaction.

As with those recruited straight from school, highlight the factors that will most appeal to those embarking on a cybersecurity career, including the possibility of a clear career path that presents opportunities for continued growth.

Conclusion

The 2019 study provides many insights into today's cybersecurity workforce, giving us clearer visibility into those professionals and their teams, helping us better define the challenges these teams face, and uncovering opportunities for organizations to take control of their cybersecurity.

While the global cybersecurity workforce gap is daunting, with real-world implications for organizations, it is not insurmountable. By estimating the global cybersecurity workforce, we know that it needs to grow by 145%. That's a number organizations can get their arms around. By recruiting talented men and women into the field, attracting experts from outside the organization, and helping to train and develop existing team members, organizations can improve their security stance and help close the gap in their corner of the world.

About (ISC)²

Celebrating its 30th anniversary this year, (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 140,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is supported by our commitment to educate and reach the general public through our charitable foundation – The Center for Cyber Safety and Education™.

For more information on (ISC)², visit www.isc2.org, follow us on Twitter or connect with us on Facebook and LinkedIn.

About the (ISC)² Cybersecurity Workforce Study

(ISC)² conducts in-depth research into the challenges and opportunities facing the cybersecurity profession. The (ISC)² Cybersecurity Workforce Study is conducted annually to assess the cybersecurity workforce gap, 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.

Sources

[1] Preimesberger, Chris, "What We Learned from Malware Attacks in 2018," eWeek, January 23, 2019.
https://www.eweek.com/security/what-we-learned-from-malware-attacks-in-2018

[2] Collier, Kevin, "Crippling ransomware attacks targeting US cities on the rise," CNN, May 10, 2019.
https://www.cnn.com/2019/05/10/politics/ransomware-attacks-us-cities/index.html

[3] Spadafora, Anthony, "Mobile malware attacks double in 2018," TechRadar, March 5, 2019.
https://www.techradar.com/news/mobile-malware-attacks-double-in-2018

[4] "Building a Resilient Cybersecurity Culture," (ISC)², 2018.
https://www.isc2.org/-/media/Files/Reports/Building-A-Resilient-Cybersecurity-Culture.ashx?la=en&hash=5BBBD1218138977BF7150E1593319F70B5670B6F