(ISC)²

Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens

(ISC)² CYBERSECURITY WORKFORCE STUDY, 2018

Table of Contents

Introduction

Awareness of the cybersecurity skills shortage has been growing worldwide. Nevertheless, that workforce gap continues to grow, putting organizations at risk. Despite increases in tech spending, this imbalance between supply and demand of skilled professionals continues to leave companies vulnerable. It's no surprise that research shows the shortage of cybersecurity professionals is now the #1 job concern among those who already work in the field.

The dynamics of the gap—including the impact on businesses and individuals—are complex. Cybersecurity touches almost everyone in an organization. Employees from Legal to Marketing, Finance to Operations, are increasingly aware of how data flows through the organization and what it takes to keep it secure. Meanwhile, IT (IT/ICT) professionals are often responsible for securing their organization's critical assets, but don't have a formal information security title. That's why (ISC)^2 is now taking a broader look at the cybersecurity field and how to address its challenges.

For the (ISC)^2 Cybersecurity Workforce Study (formerly the Global Information Security Workforce Study), we talked to cybersecurity pros as well as IT pros who spend at least 25% of their time working on cybersecurity activities. We explored the many facets of the skills gap, getting more insight into the problem and potential solutions. The survey, fielded in North America, Latin America, Asia-Pacific (APAC), and Europe, gathered input from nearly 1,500 respondents. This report explores the findings of that research, illuminating the cybersecurity skills gap by revealing the trends, elements, and impact, all of which can be used to inform the steps organizations and individual cybersecurity pros can take to address this troubling progression.

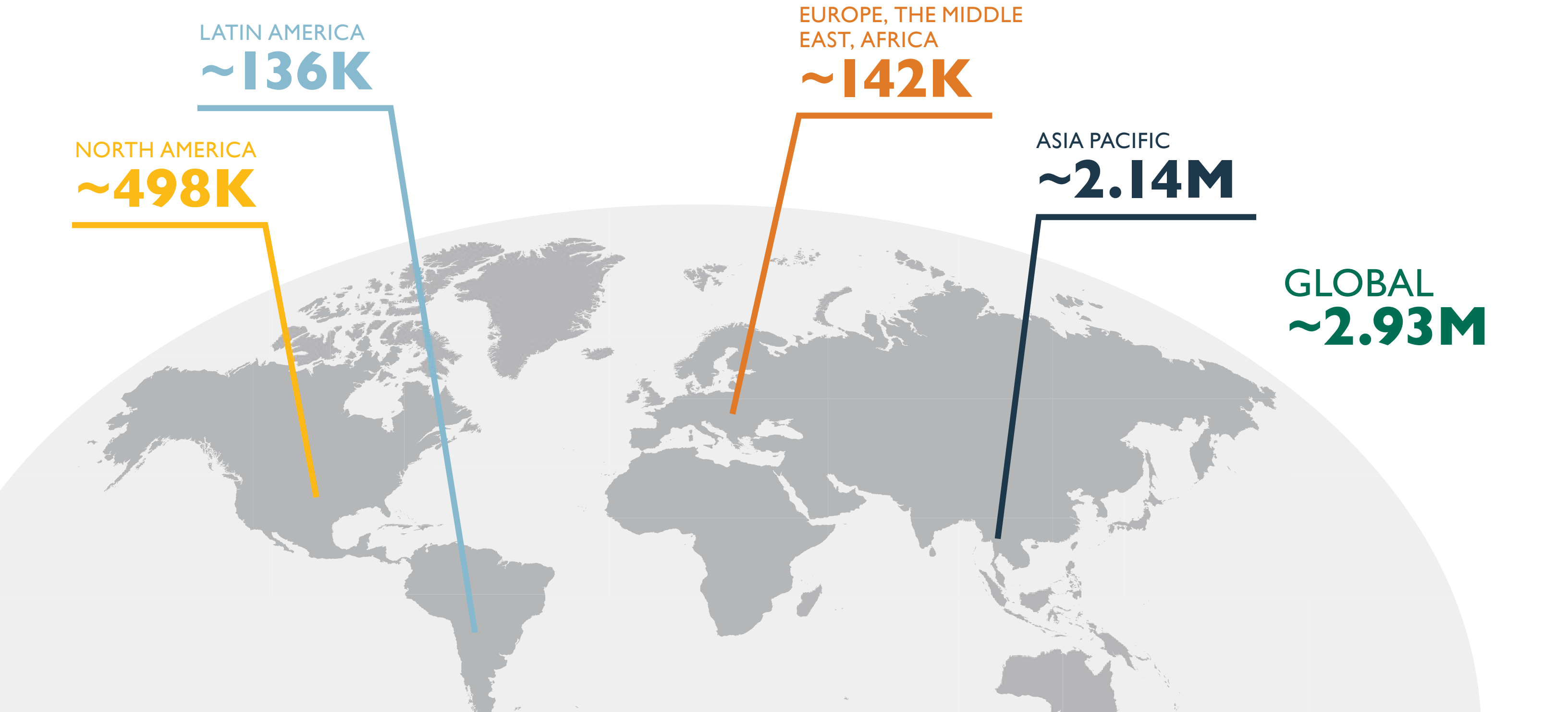
Assessing the Cybersecurity Workforce Gap

How large is the gap today? According to (ISC)^2 research, the shortage of cybersecurity professionals is close to three million globally. APAC is experiencing the highest shortage, at around 2.15 million, in part thanks to its growing economies and new cybersecurity and data privacy legislation being enacted throughout the region.

Unlike legacy gap calculation models that simply subtract supply from demand, this 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. And the calculation of supply includes estimates for academic and non-academic entrants into the field, along with estimates of existing pros 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 pros are facing worldwide.

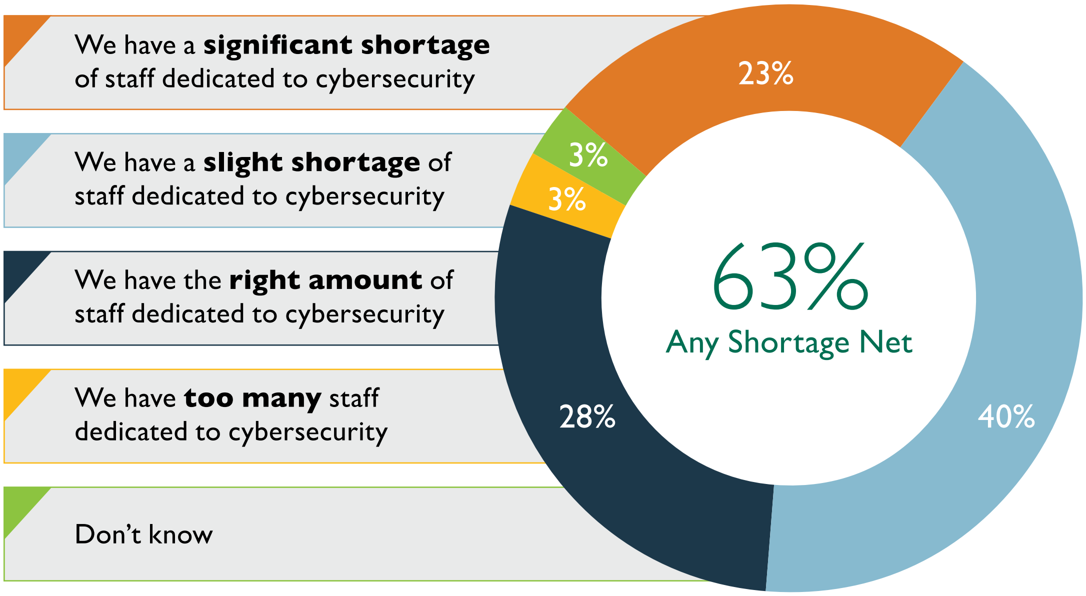
Gap in Cybersecurity Professionals by Region



The Real-World Impact of the Skills Shortage

A shortage of nearly three million: This number may seem abstract, but it's having a real-world impact on companies and on the people who are responsible for their cybersecurity. According to the survey, 63% of respondents report that their organizations have a shortage of IT staff dedicated to cybersecurity. And nearly 60% say their companies are at moderate or extreme risk of cybersecurity attacks due to this shortage.

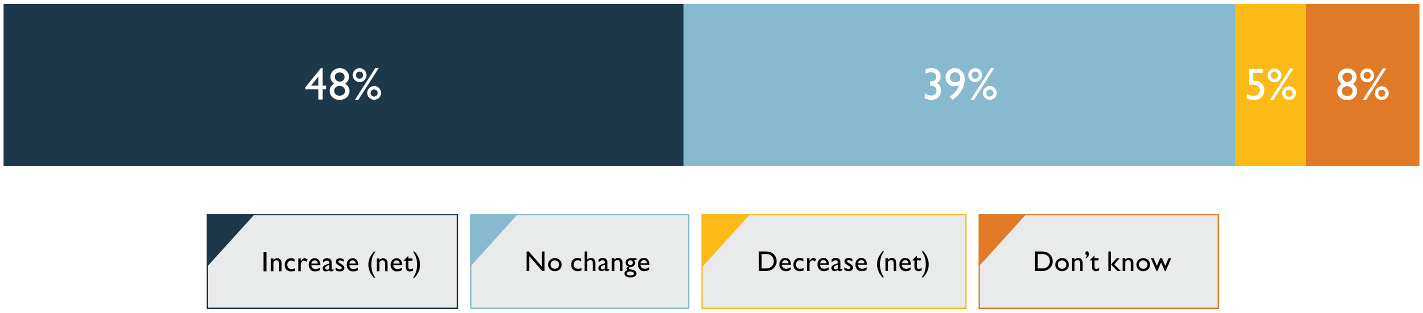
Current Cybersecurity Staffing & Level of Risk Caused by Staff Shortage



59% say their organization is at extreme or moderate risk due to cybersecurity staff shortage.

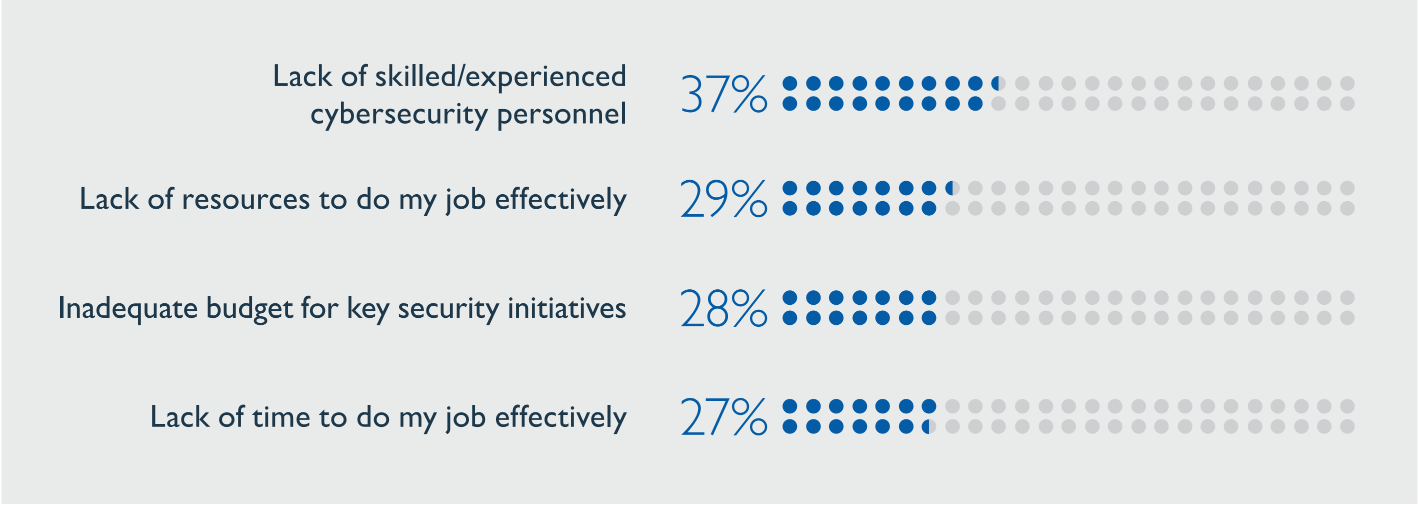
While a substantial number of companies are planning to hire more cybersecurity staff in the next 12 months, almost the same percentage expect either no change in staffing or possibly even a reduction.

Expected Change in Cybersecurity Staffing in the Next Year



How does all of this affect survey respondents? The cybersecurity workforce gap is now their #1 job concern, outranking historically topmost responses, including lack of adequate budget, lack of time and lack of work-life balance.

Top Job Concerns

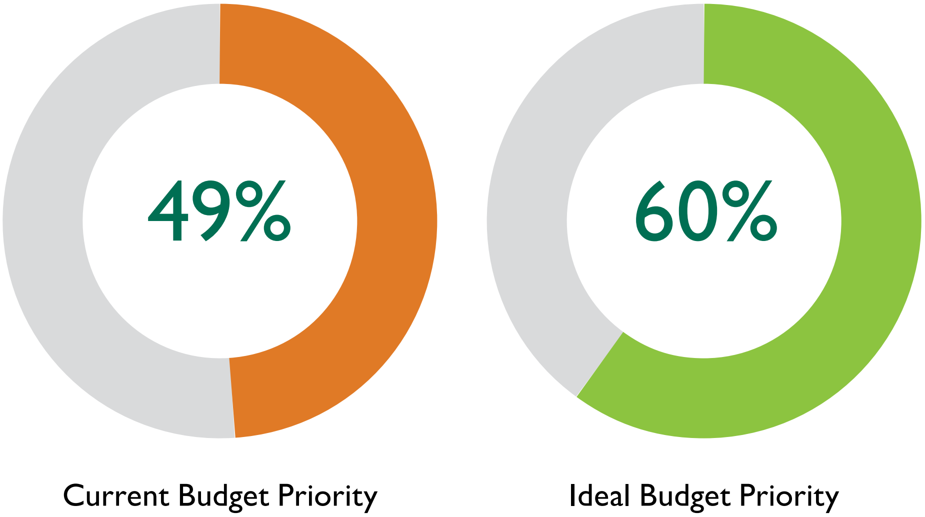


In short, the lack of skilled cybersecurity personnel is doing more than putting companies at risk; it's affecting the job satisfaction of their existing staff.

The Organization's Role in Cyber Resiliency

By supporting the people focused on cybersecurity, organizations can build more cyber resiliency across their operations. Naturally, security budgets play a role in cybersecurity preparedness and the staffing. The (ISC)² survey revealed that cybersecurity is a budget priority for companies, but cybersecurity pros consistently say that it is not a high enough priority.

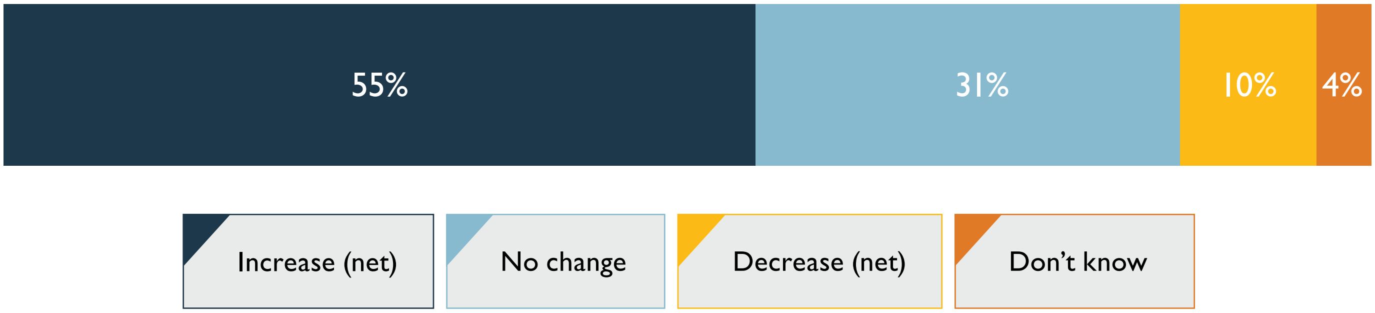
Current vs. Ideal Budget Priority for Cybersecurity



Cybersecurity is a priority for budgeting, but most professionals feel it may not be high enough. 60% say security should be a much or slightly higher budget priority.

However, more than half of the companies represented by the research expect to increase their cybersecurity budgets in the next 12 months. A solid majority of respondents, 70%, say the new amount will be a sufficient.

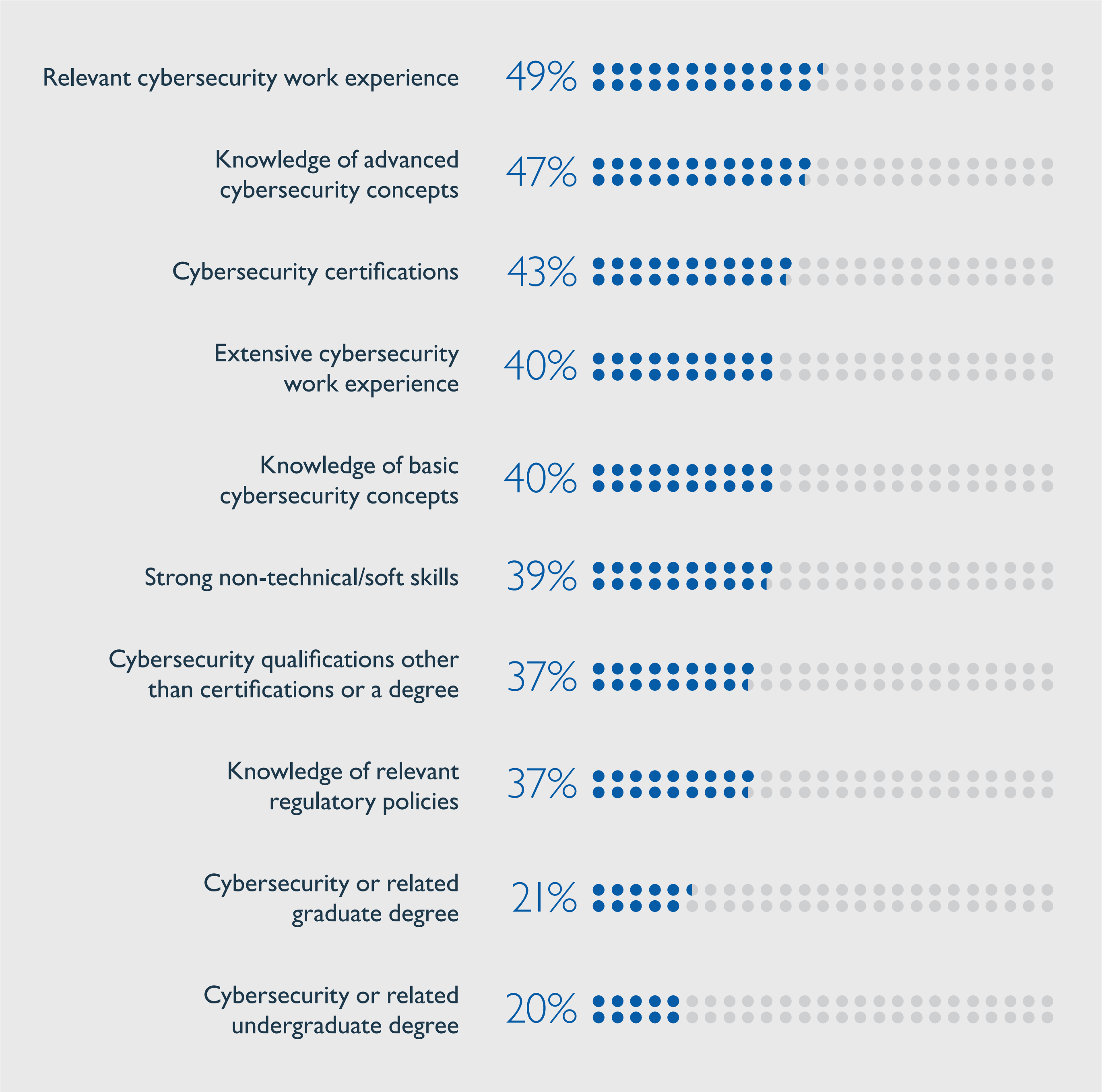
Expected Change in Cybersecurity Investments in the Next Year



When spending those budget dollars on cybersecurity hiring, companies are looking for a wide range of qualifications. Relevant work experience, knowledge of advanced cybersecurity concepts, and cybersecurity certifications are the top three. It may come as a surprise, though, that undergraduate and graduate degrees related to cybersecurity matter the *least* to hiring managers.

As professionals gain on-the-job cybersecurity work experience, organizations can help close the gap by providing more training opportunities—and focusing on the types of training that those already in the cybersecurity field find the most helpful.

Most Important Qualifications for Employment



The Cybersecurity Community: At a Glance

Who's in the cybersecurity community? (ISC)^2 research reveals the broader cybersecurity workforce is younger and more diverse than earlier research had reported.

Age/Generation:

Gen X and Baby Boomers make up 49% of the cybersecurity workforce, while Millennials and Gen Y now comprise 35% of the field.

Gender:

Women represent 24% of the cybersecurity workforce overall—a stronger representation than shown in our previous studies, thanks to our broader view of who works in the field.

Annual Salary:

Cybersecurity pros make about $85K per year, on average. Those holding security certifications have an average salary of $88K, while those without earn much less—about $67K, on average.

Reporting Structure:

Just 23% of cybersecurity pros report to security staff, while most (65%) report to C-level execs or IT directors not focused on cybersecurity.

Education:

Cybersecurity pros are well educated, with 34% reporting that they have Master's degrees and 39% having received their Bachelor's degrees.

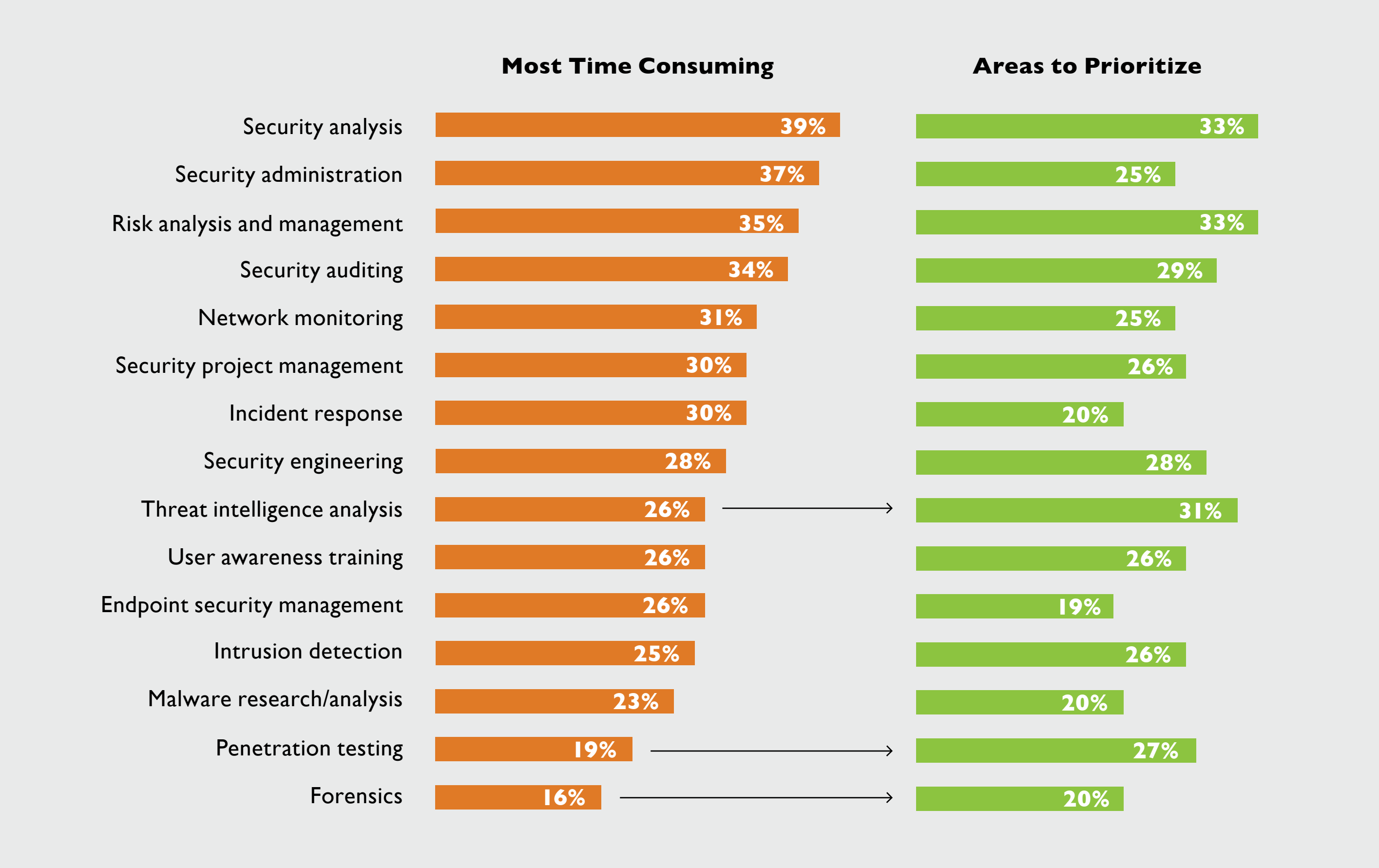
Job Tenure:

Cybersecurity pros often have had a lot of time on the job. They report having worked in an IT role for 13 years, on average, and seven years on cybersecurity initiatives.

The Perspective from the Trenches

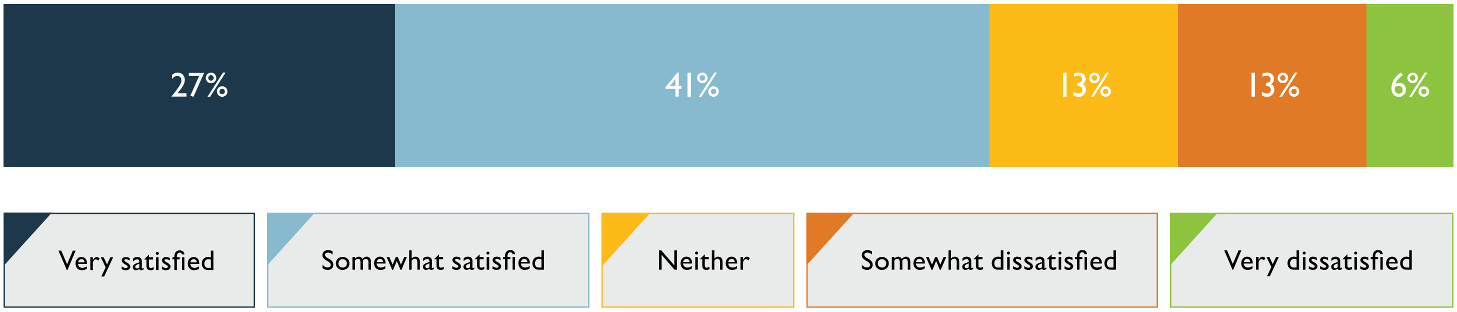
Today's cybersecurity pros have an instructive story to tell—one that can be informative for others in the field, as well as for companies feeling the pain of the skills shortage. And the story begins with how cybersecurity pros spend their day. While many cybersecurity tasks are simply necessary evils, there are some tasks that they would like to spend less time on and others that they would like to focus more on.

Security administration, incident response and endpoint security management fall in the first category. They're time-consuming activities that cybersecurity pros would like to do less of. They'd rather be spending time on more high-value cybersecurity tasks such as threat intelligence analysis, penetration testing and forensics.



How cybersecurity pros spend their time, of course, impacts their job satisfaction rates, which the survey also captured. Despite professionals looking to shift priorities, as well as other concerns and challenges, 68% of respondents say they are somewhat or very satisfied with their jobs.

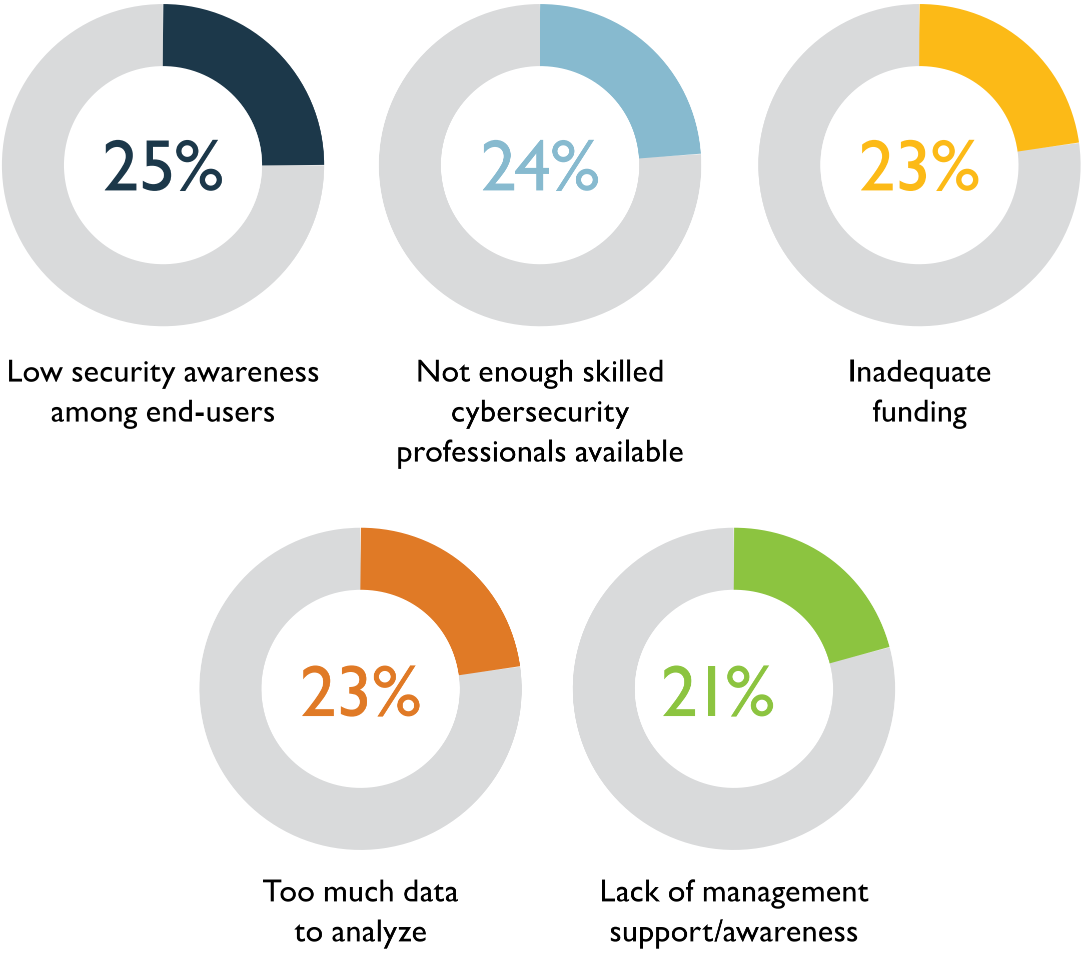
Current Job Satisfaction



By providing the right security resources, whether that means additional personnel, training or specialized cybersecurity solutions, companies can have a major impact on how cybersecurity pros spend their time, which in turn impacts their job satisfaction rates.

While dealing with day-to-day responsibilities, cybersecurity pros are also thinking long-term and considering how to progress in their careers. In the process, they are running into a few common challenges that could be addressed at the company level. For example, many of them still cite the lack of security awareness among end-users, which can lead to more security vulnerabilities. In addition to a lack of funding, the people surveyed feel that there aren't enough skilled staff available—and there's a general lack of support/awareness from management about the urgency of cyber-security initiatives overall.

Top Challenges Preventing Focus on Key Cybersecurity Initiatives



In addition, cybersecurity pros are hindered by the costs associated with training and certifications. While some companies cover the costs for professional development, the costs can be challenging for those trying to enter the field. In spite of this, these individuals understand the value the right certification can have for their career development, and more than half of all respondents globally (54%) are either pursuing cybersecurity certifications or plan to within the next year.

Top Career Progression Challenges

34%
Unclear career path opportunities in cybersecurity roles

32%
Lack of knowledge by organizations about cybersecurity skills

32%
Cost of cybersecurity certifications

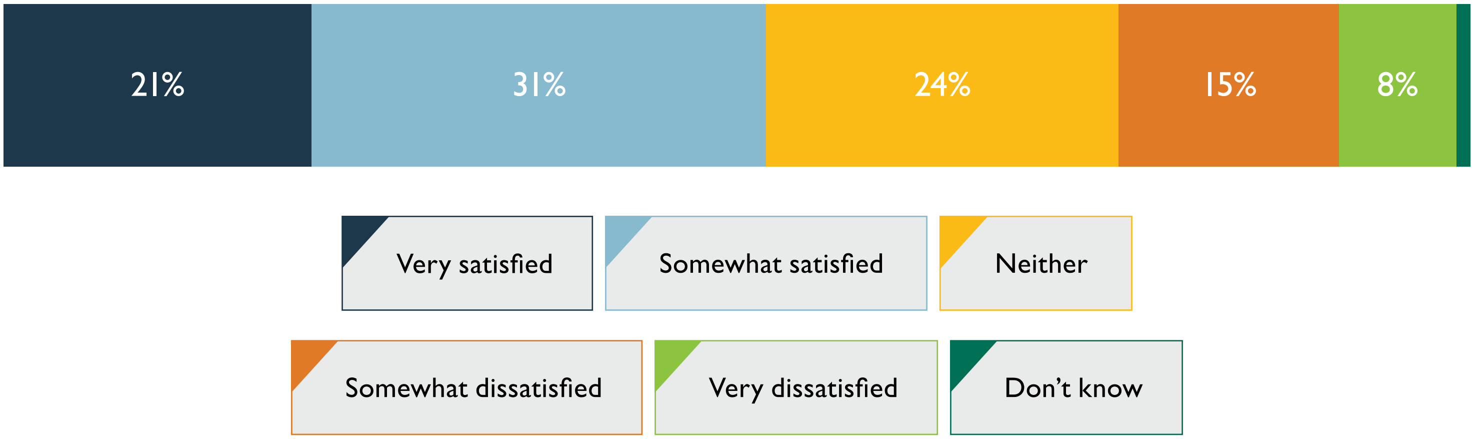
28%
Cost of formal education to properly prepare for career in cybersecurity

26%
Not enough job experience in an cybersecurity role

Whether companies are supporting training and certification efforts, or cybersecurity pros are pursuing them independently, one obstacle rises to the top. They all report that they need more time carved out for professional development. Again, companies have an opportunity to step up in ways that have a meaningful influence on cybersecurity operations.

Within companies that do provide training, about half of cybersecurity pros are either somewhat or very satisfied with the level of training resources provided. That said, these ratings leave significant room for improvement as more than one-fifth are either very or somewhat dissatisfied.

Satisfaction with Educational Resources Provided by Organization



One final area that affects job satisfaction is the lack of standardization around the cybersecurity profession as a whole. Security teams are structured differently at different companies. Workers have different titles and responsibilities. And they use different terminology and often lack a common frame of reference. This complexity is an often-overlooked frustration within the cybersecurity community.

Focusing on Professional Development

To overcome the many challenges to cybersecurity, the people working in the field are continually looking for ways to learn from best practices and fine-tune their skills. Professional development is an ideal tool for keeping up with the rapid changes in cybersecurity—and turning the job into an exciting career opportunity.

When it comes to professional development in the workplace, (ISC)^2 research revealed a sizable disconnect between what survey respondents find most beneficial and what companies are offering. Respondents ranked face-to-face, instructor-led training as the most valuable; however, that method was fifth on the list of training resources companies provide.

Most Valuable Educational Methods

Face-to-face, instructor-led training	35%
Internet-based training	31%
Conference attendance	28%
Personal study review	26%
Virtual classroom instructor-led	25%

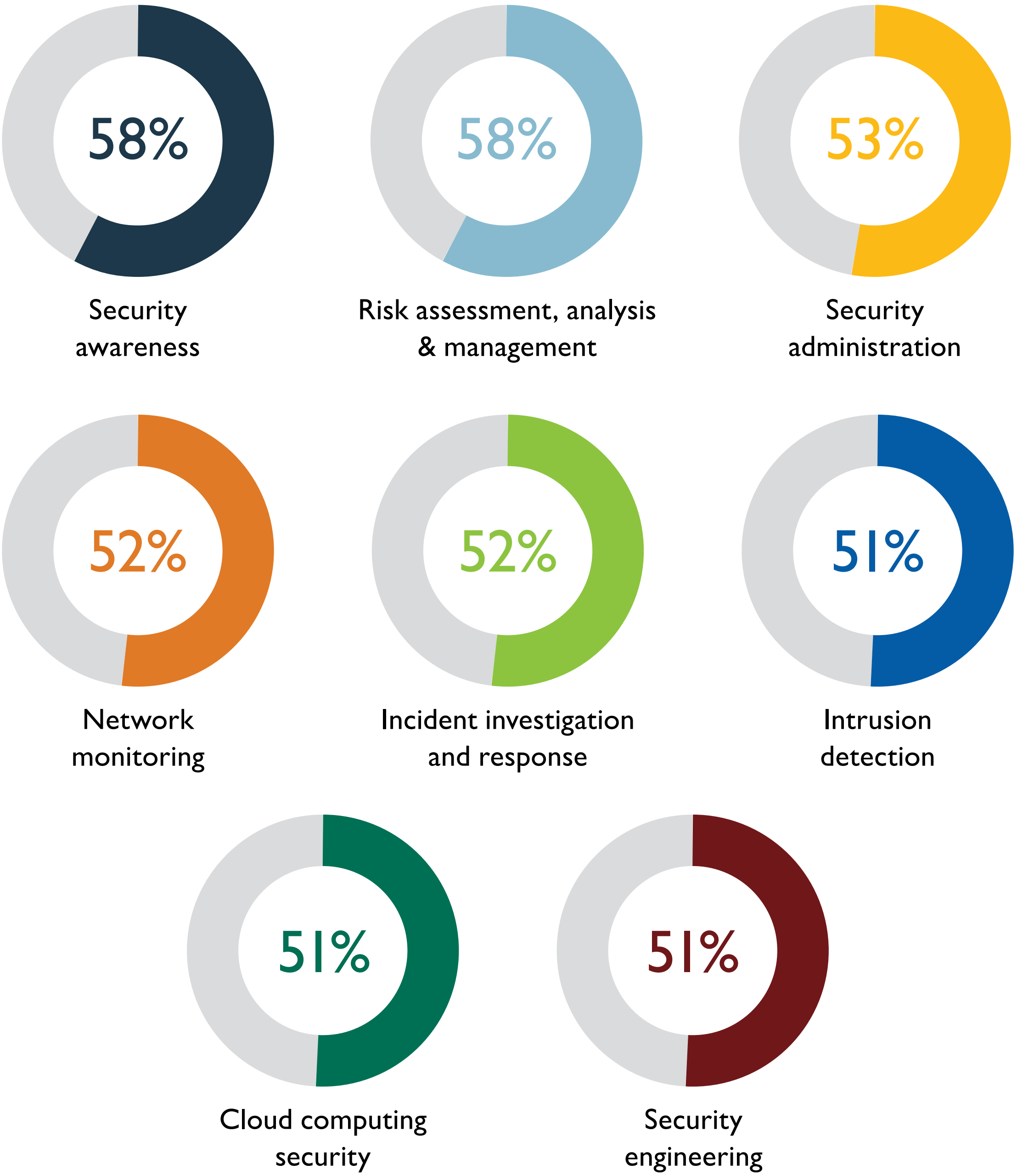
Educational Resources Offered by Organization

Internet-based training	38%
Conference attendance	31%
Personal study review	30%
On the job with peers	29%
Face-to-face, instructor-led training	27%

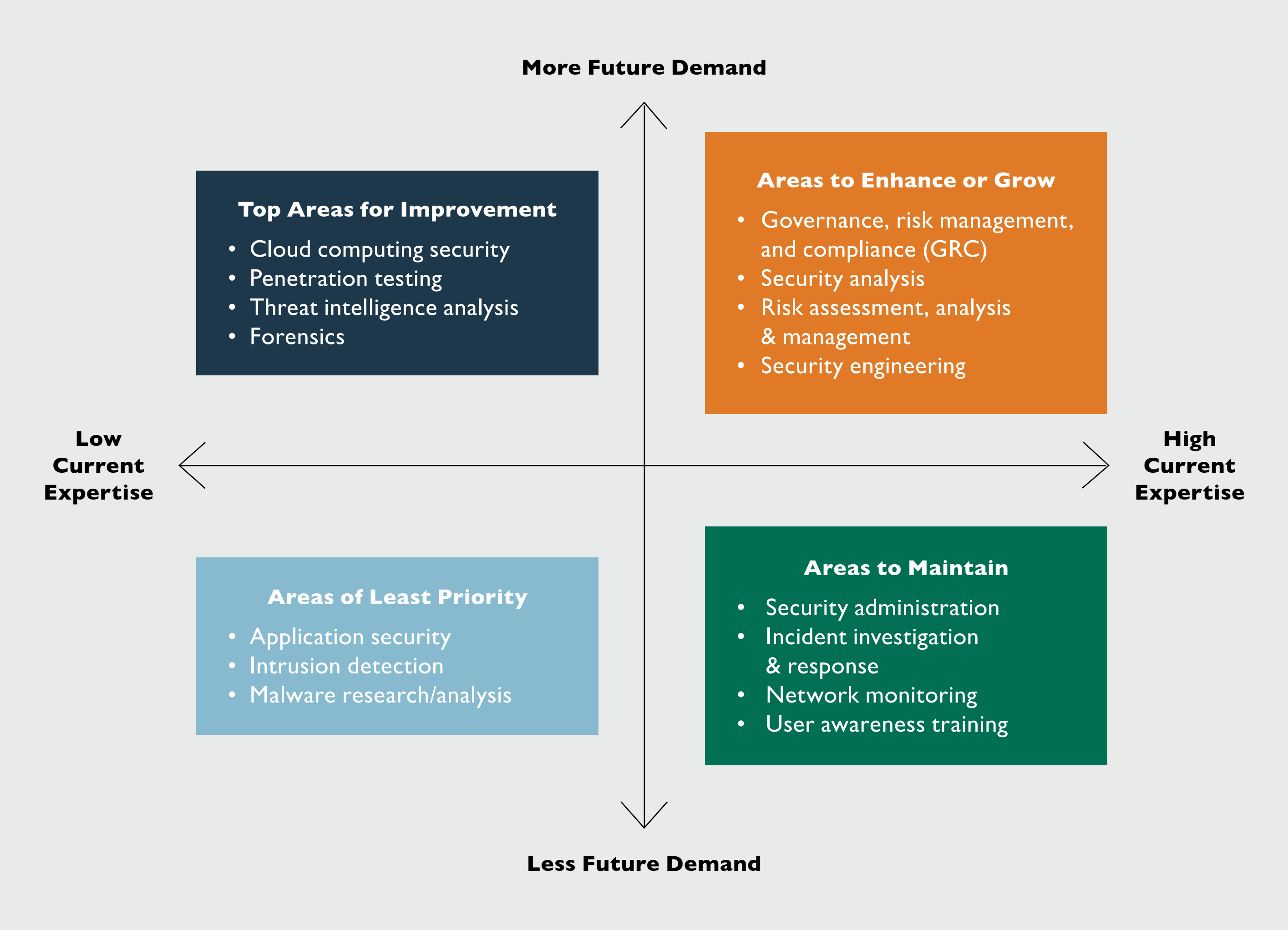
Where should the training focus? The (ISC)^2 survey revealed eight areas that more than half the cybersecurity pros surveyed feel are critical to being competitive in their field. These include security analysis, risk assessment, incident investigation and response, intrusion detection and cloud computing security.

Top Needed Cybersecurity Areas of Expertise

Showing % saying 'Critical'



In addition, the survey also looked at the areas cybersecurity pros feel they will need to develop or improve on over the next two years in order to advance in their careers. The respondents also rated themselves on their level of expertise in each area. An analysis of the results revealed the areas cybersecurity pros need to enhance and maintain based on higher future demand, areas for improvement based on low levels of experience, and areas of least priority based on lower future demand.



Top Areas for Improvement

- Cloud computing security
- Penetration testing
- Threat intelligence analysis
- Forensics

Areas to Enhance or Grow

- Governance, risk management, and compliance (GRC)
- Security analysis
- Risk assessment, analysis & management
- Security engineering

Areas of Least Priority

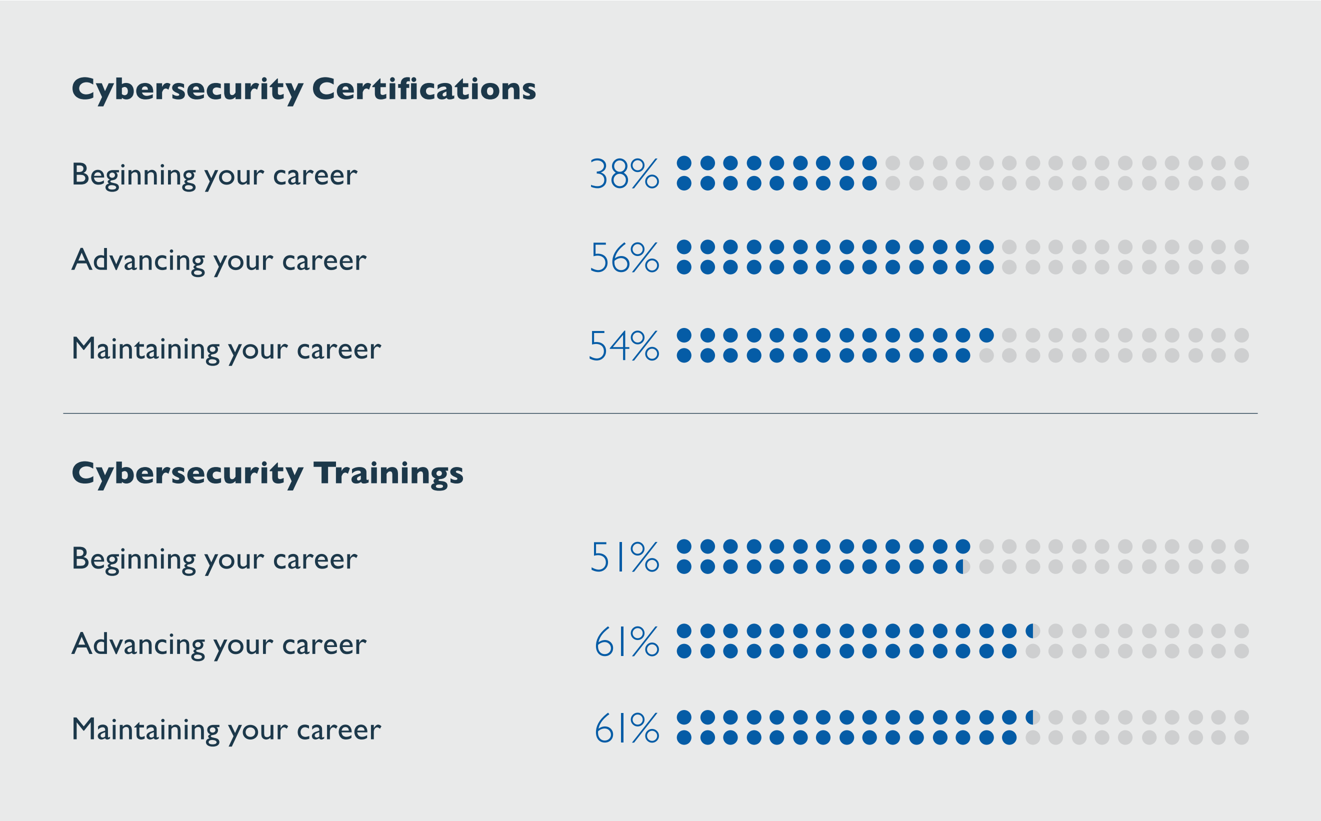
- Application security
- Intrusion detection
- Malware research/analysis

Areas to Maintain

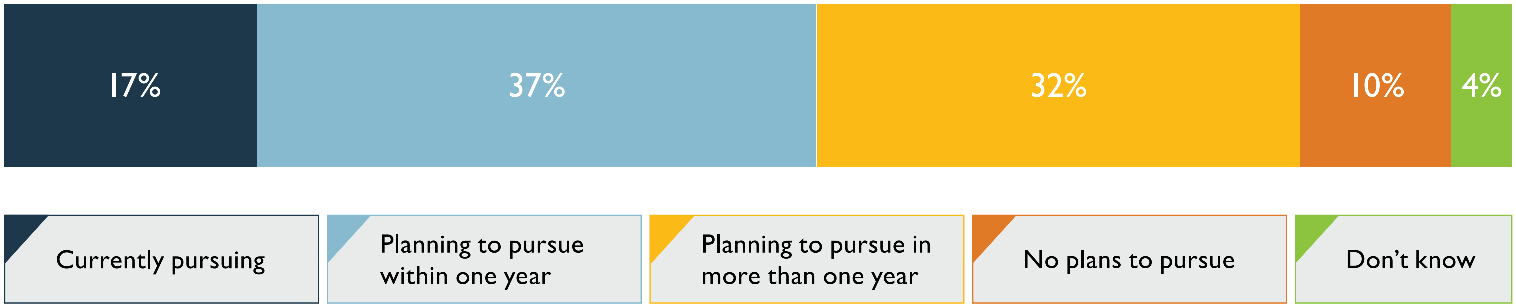
- Security administration
- Incident investigation & response
- Network monitoring
- User awareness training

Along with pursuing these and other cybersecurity skillsets, a majority of the survey's respondents say that cybersecurity certifications and training are important for maintaining and advancing their careers. The vast majority, 86%, are either currently pursuing cybersecurity certifications or planning to in the future.

Importance of Certifications/Trainings



Cybersecurity certifications are seen as the most important for advancing and maintaining careers.



Many professionals are currently pursuing cybersecurity certifications or plan to within the next year.

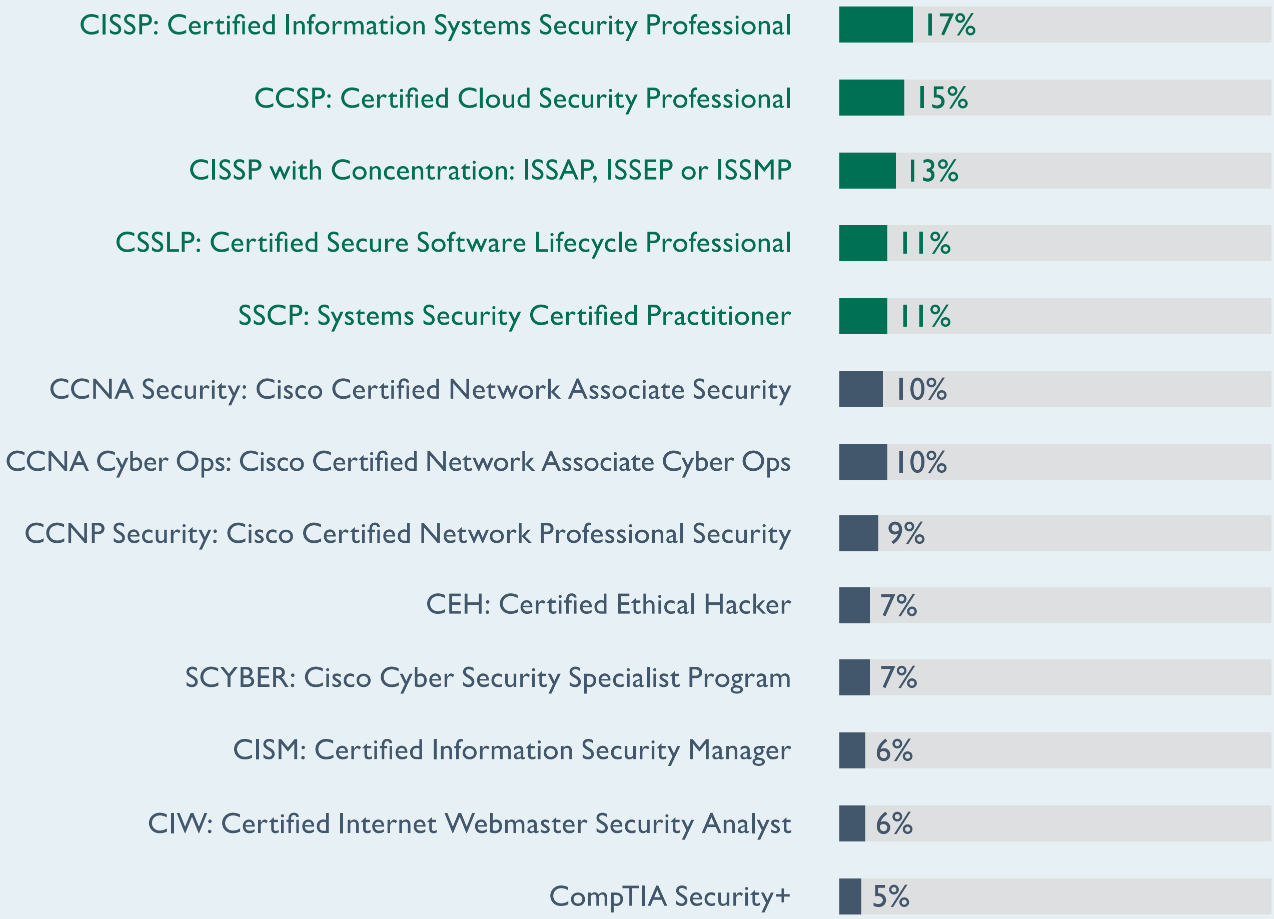
Certifications and Professional Memberships

Cybersecurity pros are actively working on improving their careers, and here's how we know it.

Security Organization Membership: 1/3 of the survey respondents belong to (ISC)^2, while 17% are members of CompTIA, followed by the Cloud Security Alliance (CSA) and Information Systems Security Association (ISSA).

IT Security Certifications: 27% of cybersecurity pros are Certified Information Systems Security Professionals (CISSPs). Other top certifications include BS 7799/ISO 27001 ISMS Auditor, Cisco Certified Network Associate (CCNA) Security, and CompTIA Security+.

Upcoming Certifications: In the next 12 months, the top security certifications cybersecurity professionals plan to pursue are:



Conclusion

As cybersecurity pros around the globe work to gain and enhance their skillsets, organizations can help support these people on the frontlines of securing the cyber world. Companies who employ new recruits should explore options available for training them for the job and setting them up for success. They also need to provide more professional development opportunities for the people who already work in cybersecurity—and allow sufficient time for their staff to pursue them. Investing in current team members can be a highly cost-effective way to shore up cybersecurity skills in an organization.

Finally, as they increase their security budgets, companies must portion out those funds mindfully, combining investments in personnel, training and security solutions to create a comprehensive cybersecurity approach that can shrink their piece of the gap.

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 (formerly the Global Information Security 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.

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, programmatic approach to security. Our membership, over 138,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry.

For more information on (ISC)², visit www.isc2.org.

Methodology

(ISC)² commissioned Spiceworks to conduct a survey in August 2018. This survey targeted cybersecurity professionals worldwide to measure the gap in the cybersecurity workforce in companies of all sizes and to understand current perceptions and practices around cybersecurity. Survey results included responses from approximately 1,452 participants throughout North America, Latin America, Asia-Pacific and Europe.

(ISC)²®