MARKET RESEARCH

(ISC)² Cybersecurity Hiring Managers Guide

Best Practices for Hiring and Developing Entry- and Junior-Level Cybersecurity Practitioners

(ISC)²® Inspiring a Safe and Secure Cyber World

INTRODUCTION

Cybersecurity is a high-demand, high-profile profession with acute staffing shortages. Facing a fierce recruiting environment, successful hiring managers have learned to be more creative and flexible as they strive to build resilient, sustainable cybersecurity teams. New research by (ISC)² finds that hiring managers are looking to entry- and junior-level candidates to fill vacancies, take on everyday duties, and add value and fresh new perspectives that help strengthen security operations.

The cybersecurity skills gap currently stands at 2.7 million globally[1]. Previous (ISC)² research[2] suggests organizations must look outside the traditional pool of cybersecurity candidates to build resilient teams at all skill levels. Finding and nurturing newcomers to the field requires a shift in recruiting tactics and an investment in training to enable new hires to learn and grow.

91% of Hiring Managers Offer Professional Development During Work Hours

Findings underscore there is no single pathway into cybersecurity. Hiring managers must be resourceful in finding entry- and junior-level candidates, and carefully determine the appropriate tasks to assign.

Businesses know that to be successful, they must invest in people; we found 91% of study participants' organizations allow entry- and junior-level staff development time during work hours. For most organizations, the cost of development is relatively low, ranging from U.S. $500 to $5,000. Research also reveals it doesn't take long for entry- and junior-level practitioners to be "up to speed." 37% of hiring managers we spoke to said entry- and junior-level hires are ready to handle assignments independently within six months or less on the job.

[1] The 2021 (ISC)² Cybersecurity Workforce Study
[2] The (ISC)² Cybersecurity Career Pursuers Study

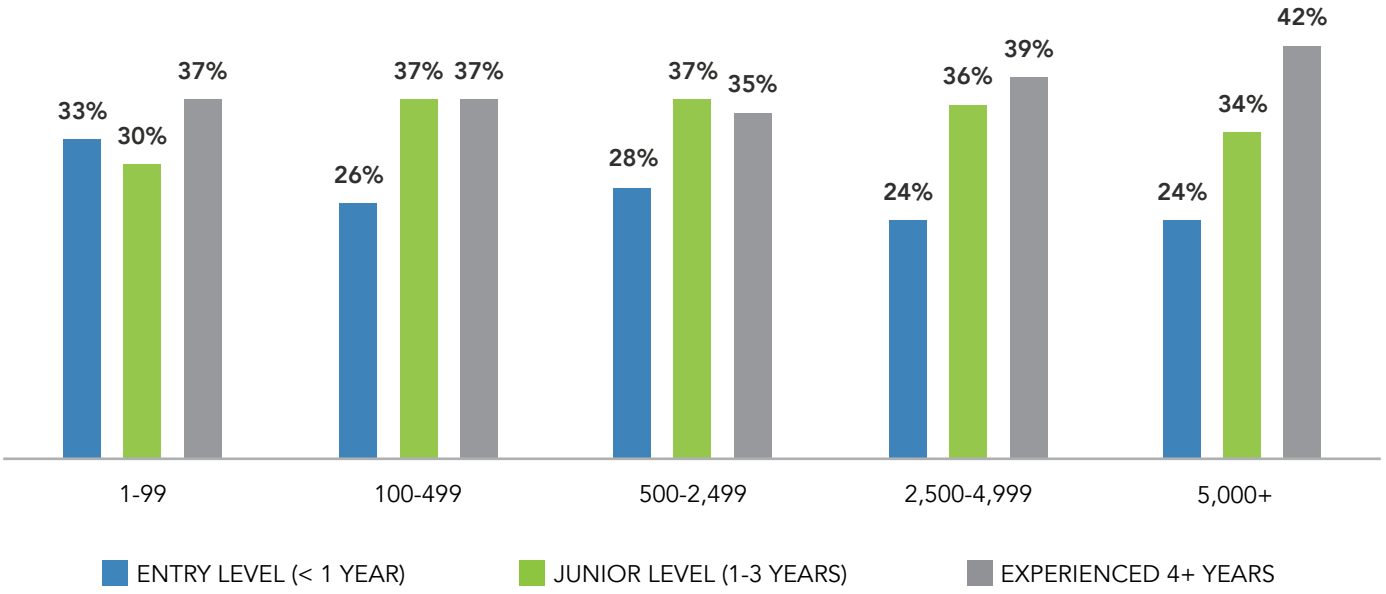
Who We Spoke To

Because finding experienced candidates for cybersecurity positions remains a top challenge for many organizations, (ISC)² set out to learn how hiring managers recruit and support the career development of entry- and junior-level practitioners. Our objective was to gain insights into successful hiring practices, and to learn how long onboarding and initial training typically takes and the financial investments needed.

(ISC)² polled 1,250 hiring managers at small, mid-size and large organizations in the United States, Canada, United Kingdom and India about their practices and preferences. All study participants are responsible for hiring entry- and junior-level roles at their organization, with 91% of them having hired staff at this experience level within the last two years. For the purpose of this study, entry-level team members are defined as staff with less than one year of experience, while junior-level practitioners are defined as having one to three years of experience. A third category of "experienced" (four or more years of experience) was also used for comparison purposes.

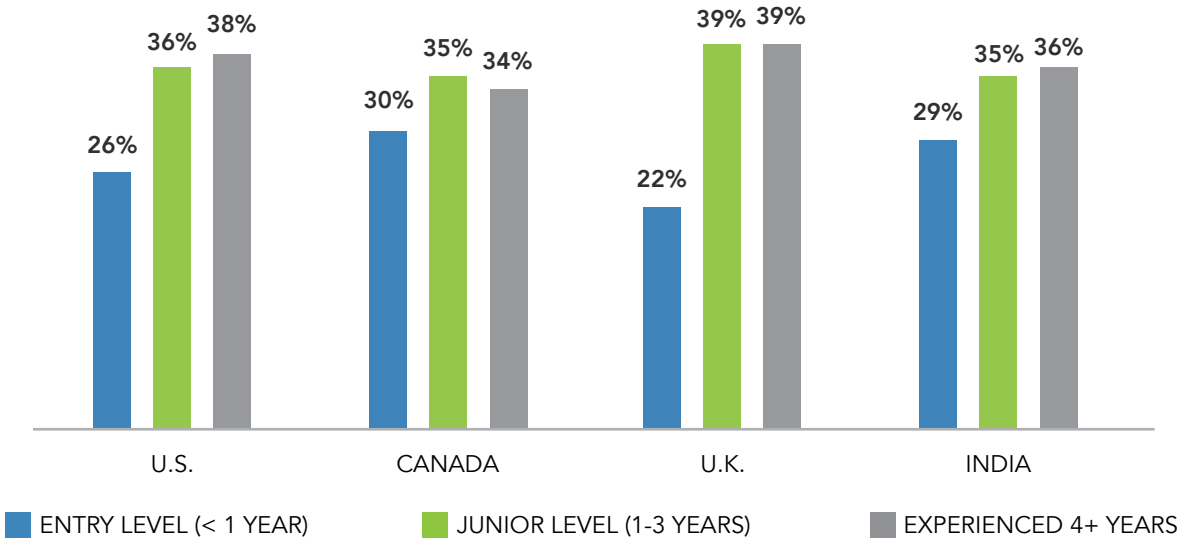
Security Team Composition by Experience Level by Organization Size

(Number of Employees)



Entry- and junior-level practitioners combined make up nearly two-thirds of participant organizations' security teams on average. Larger organizations tend to have higher percentages of more experienced professionals on their security teams.

Team Composition by Experience Level by Country



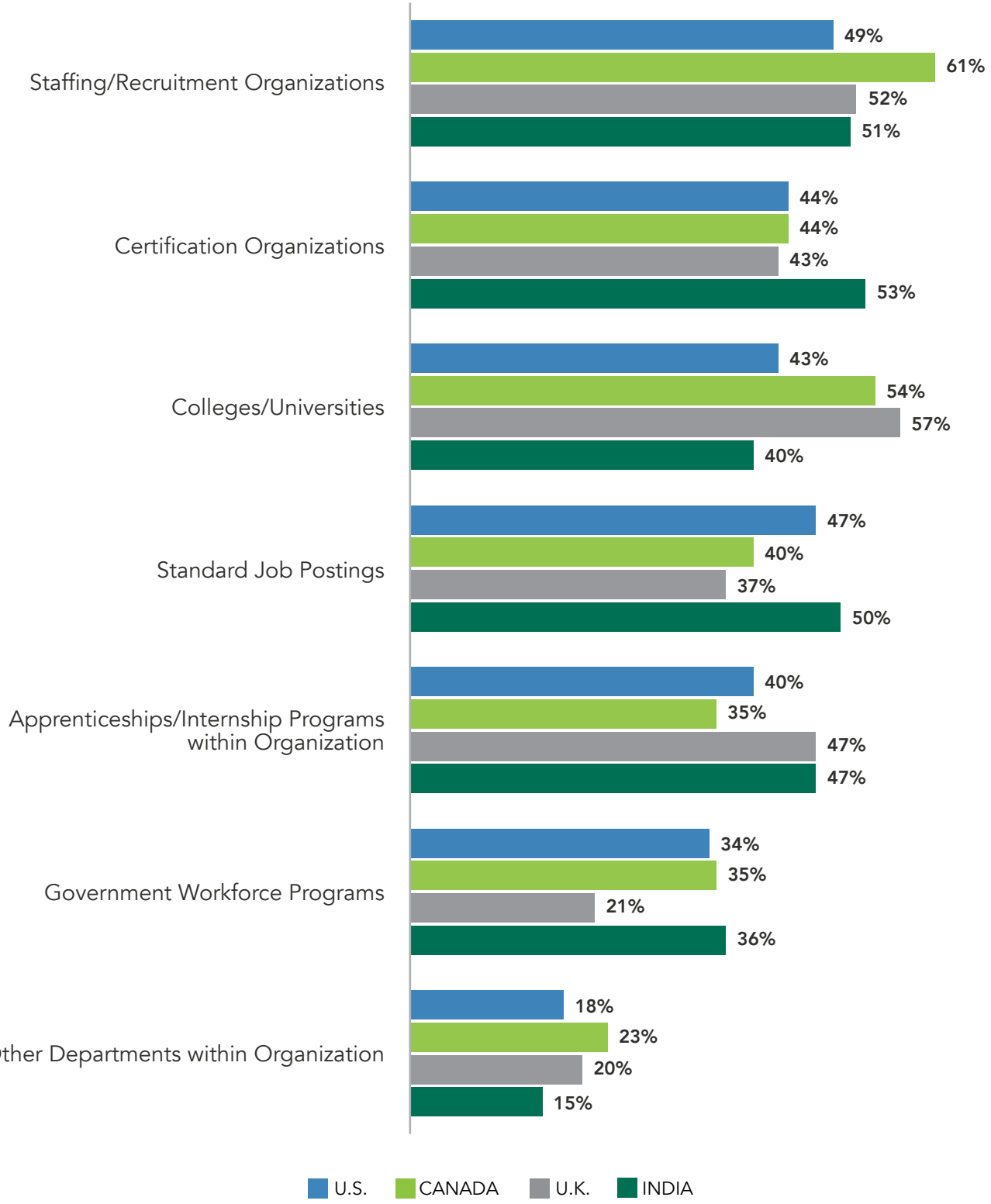
We found relatively consistent team composition by experience level across regions with only a few exceptions. Security teams in the U.K. had the lowest percentage of entry-level staff, while hiring managers in Canada and India reported the highest.

Many Paths to Cybersecurity Careers

The first step to hiring promising team members is figuring out where to find them. The most popular method, cited by 52% of study participants, is to work with staffing and recruitment organizations. This approach is followed by looking to certification organizations (46%), and colleges and universities (46%). Managers also rely on standard job postings (45%) to find candidates; apprenticeships and internships within their own organizations (43%); and partnerships with government workforce programs (33%).

The study found variations in hiring practices between regions and industries. For instance, managers in manufacturing rely on educational institutions at the highest rate, while those in software and hardware development prefer recruiters, and those in IT services favor workforce programs. Canadian and U.K. hiring managers rely more on partnerships with educational institutions for entry- and junior-level candidates than their counterparts in the U.S. and India. For its part, India favors certification organizations at the highest rate.

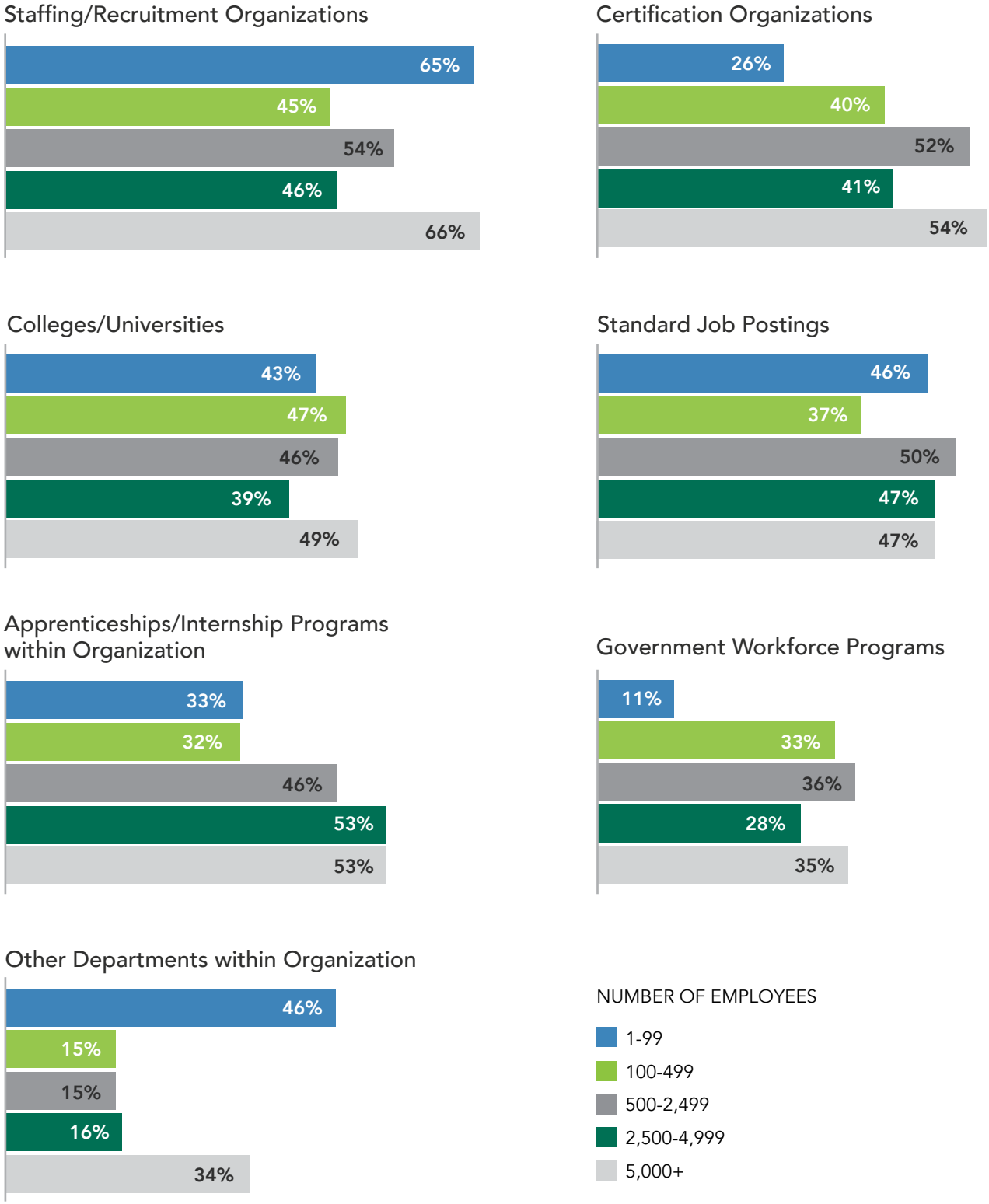
How Hiring Managers Find Entry- and Junior-Level Talent by Country



Hiring managers rely on a wide array of tactics and resources to hire entire entry- and junior-level staff. While recruitment firms and certifying bodies rank high across all countries, apprenticeships and internships are more popular in the U.K. and India.

How Hiring Managers Find Entry- and Junior-Level Talent by Organization Size

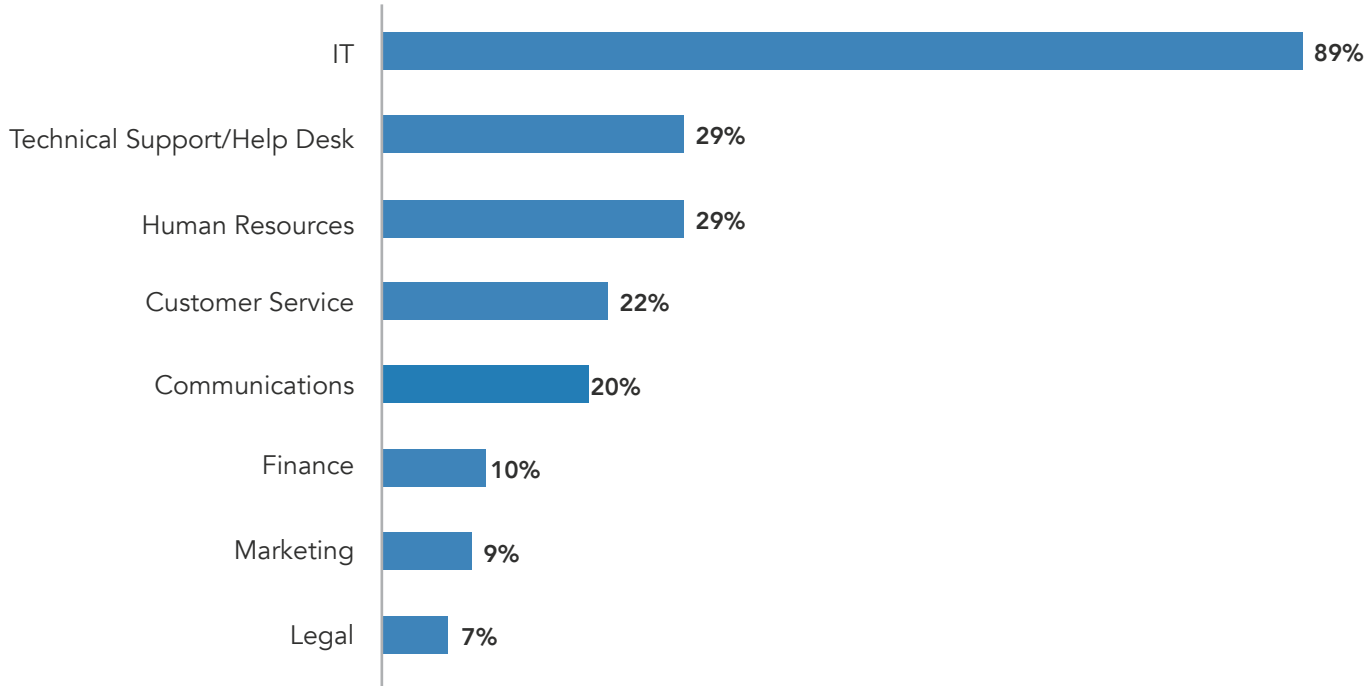
(Number of Employees)



Larger organizations are reaping the benefits of internship and apprenticeship programs, which provide entry- and junior-level practitioners with hands-on experiences and exposure to a career in cybersecurity.

A less-used option is hiring individuals from within the organization working in different job functions, which was only used by 18% of study participants. 46% of organizations with fewer than 100 people and 34% of those with more than 5,000 employees, say they recruit entry- and junior-level staff from other departments.

Where to Find Entry- and Junior-Level Talent Inside Your Organization



Hiring managers find staff with transferable skills within IT departments. However, they also find talent outside of IT, which (ISC)² research[3] confirms is an increasingly less prominent career pathway into cybersecurity, especially among younger professionals, women and other under-represented groups.

[3] The 2021 (ISC)² Cybersecurity Workforce Study

BUILDING ENTRY-LEVEL JOB DESCRIPTIONS IS A TEAM EFFORT

The dreaded kitchen-sink, all inclusive, unrealistic entry-level job description continues to be derided as a major cause of organizations' cybersecurity staffing challenges. Our research suggests more collaboration between hiring managers and HR is the solution. Participants — who make hiring entry-level positions a priority — tell us that creating job descriptions is a shared responsibility among cybersecurity hiring managers, their teams and human resources.

Who Takes the Lead?

	Human Resources	Cybersecurity Managers	Cybersecurity Teams
Critical and Required Technical Skills	36%	67%	46%
Nice to Have Technical Skills	37%	62%	50%
Non-Technical Skills and Personality Attributes	51%	52%	45%
Education Requirements	46%	64%	46%
Certification Requirements	35%	63%	51%
Professional Experience Requirements	36%	66%	52%
Security Clearance and Compliance Requirements	32%	62%	54%

We asked participants who at their organizations contribute to the various components of entry-level job descriptions. Our study reveals that building effective job descriptions seems to be a collaborative effort between managers, their teams and HR to determine the technical and non-technical requirements needed to attract candidates.

Moreover, our research uncovered an extensive list of tasks and responsibilities hiring managers assessed across experience levels (see page 15). This can help guide hiring managers as they identify the key tasks and responsibilities by job type and experience level that newcomers can be expected to learn and perform. Being clear, consistent and reasonable about assigned tasks and responsibilities sets expectations for hiring managers and new hires to avoid misunderstanding and potential frustration in the future.

TOP TASKS IDENTIFIED FOR ENTRY-LEVEL CANDIDATES INCLUDE:

35% Alert and Event Monitoring

35% Documenting Processes and Procedures

29% Using Scripting Languages

28% Incident Response

26% Reporting (Developing and Producing Reports)

Disconnects still exist, though, when evaluating realistic qualifications for entry- and junior-level roles. When asked which certifications help identify ideal entry- and junior-level candidates, hiring managers cited certifications requiring several years of experience. The (ISC)² Certified Information Systems Security Professional (CISSP) received the most mentions, followed by the ISACA Certified Information Security Manager (CISM) certification – both credentials are designed for experienced cybersecurity professionals.

How have entry- or junior-level cybersecurity team members helped your organization?

"They have come to work with fresh ideas. Things they may have learned while in school and new technologies that may not have hit the mainstream yet."

What Hiring Managers Value Most

Previous research has highlighted challenges identifying qualified cybersecurity jobseekers. The tendency for many organizations is to seek candidates with the highest technical qualifications and relevant certifications, but expecting those qualifications is unrealistic for entry- and junior-level candidates.

As the (ISC)² Cybersecurity Career Pursuers Study[4] demonstrated, technical skills aren't the only important attributes a candidate can offer. Among other talents, creative and analytical thinking, teamwork, and the ability to work independently and in a team are important. The (ISC)² Cybersecurity Workforce Study[5] affirms this as cybersecurity professionals believe traits such as strong problem-solving abilities, curiosity and eagerness to learn, strong communication skills, and strategic thinking are equally or more important than certifications and relevant cybersecurity experience.

We asked hiring managers to rate a broad range of technical and non-technical skills, to produce weighted Top Lists of what they are looking for in entry- and junior-level candidates. The study confirms hiring managers view a range of technical and non-technical attributes as indicators of cybersecurity career success.

[4] The (ISC)² Cybersecurity Career Pursuers Study
[5] The 2021 (ISC)² Cybersecurity Workforce Study

LOOK FOR THESE TRAITS WHEN HIRING ENTRY- AND JUNIOR-LEVEL TEAM MEMBERS

TOP 5 TECHNICAL SKILLS

1. Data Security
2. Cloud Security
3. Secure Software Development
4. Data Analysis
5. Security Administration

TOP 5 NON-TECHNICAL SKILLS

1. Ability to Work in a Team
2. Ability to Work Independently
3. Project Management Experience
4. Customer Service Experience
5. Presentation Skills

TOP 5 PERSONALITY ATTRIBUTES

1. Problem Solving
2. Creativity
3. Analytical Thinking
4. Desire to Learn
5. Critical Thinking

Hiring managers in our study look beyond technical abilities to uncover top non-technical attributes and skills they identify as strong indicators of future cybersecurity career success.

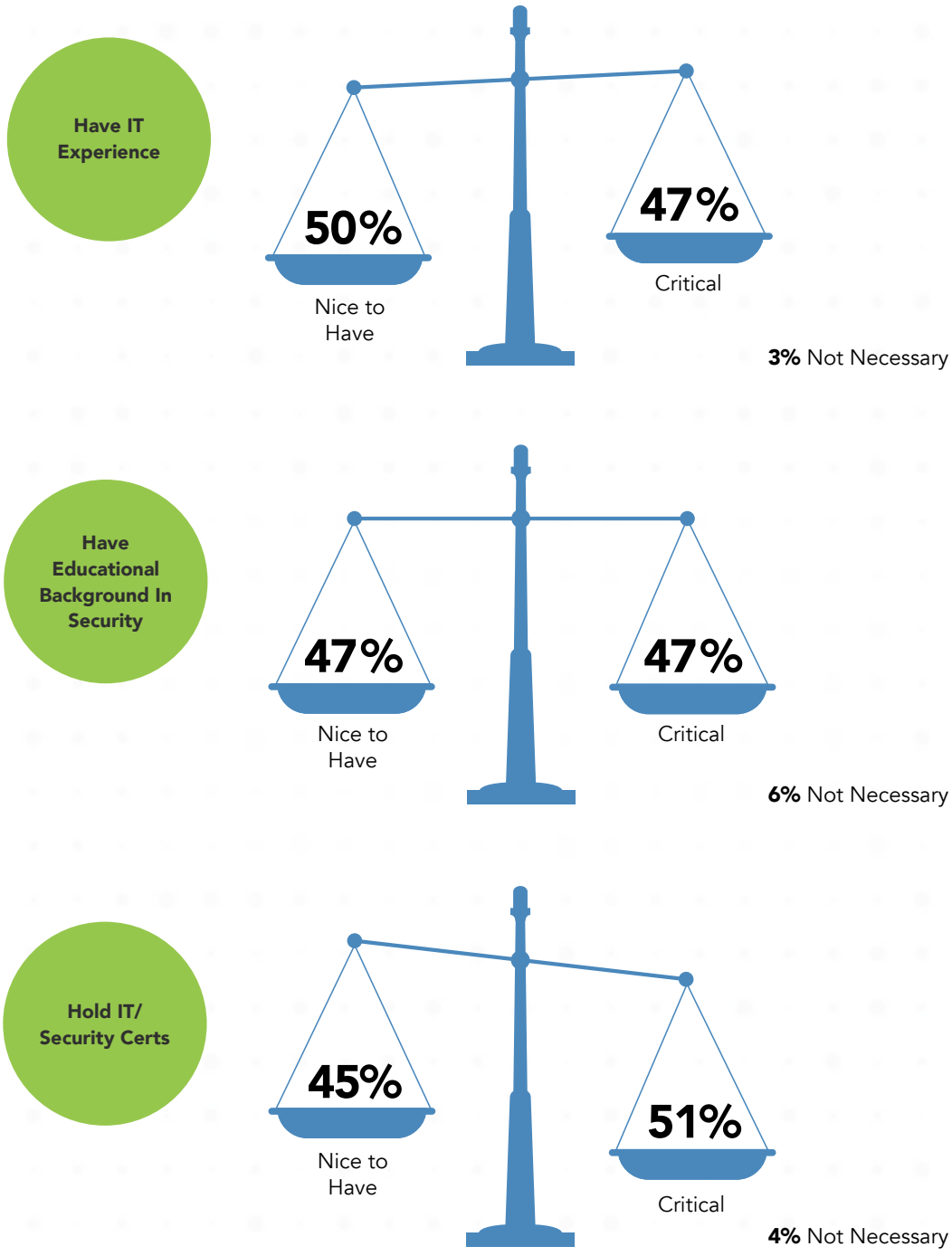
How have entry- or junior-level cybersecurity team members helped your organization?

"Fresh ideas and perspectives. Willingness to go the extra mile to learn and get ahead."

IT Experience Not Always the Winning Attribute

Our research also reveals an openness to considering entry- and junior-level candidates without IT experience. When asked how important it was for candidates to have IT experience, have an education background in security or hold IT/security certifications, participants were nearly evenly split as to whether each attribute was critical or just a "nice to have" as an indicator of a successful candidate.

Balancing the Importance of IT Experience, Education and Certifications



Times are changing for hiring managers focused on recruiting entry- and junior-level staff. In the search for talent, hiring managers are balancing expectations for certifications, college degrees and IT experience with broader assessments of what qualities and attributes signal strong candidates who can contribute early and learn on the job. Attaining certifications and ongoing professional development remain important for future growth.

Learning on the Job

On the job training is critical for entry- and junior-level staff, and our research revealed those tasks most likely to be assigned to each experience level.

TOP 5 TASKS FOR ENTRY-LEVEL STAFF (Less than 1 Year of Experience)

- **35%** Alert and Event Monitoring
- **35%** Documenting Processes and Procedures
- **29%** Using Scripting Languages
- **28%** Incident Response
- **26%** Reporting (Developing and Producing Reports)

TOP 5 TASKS FOR JUNIOR STAFF (1-3 Years of Experience)

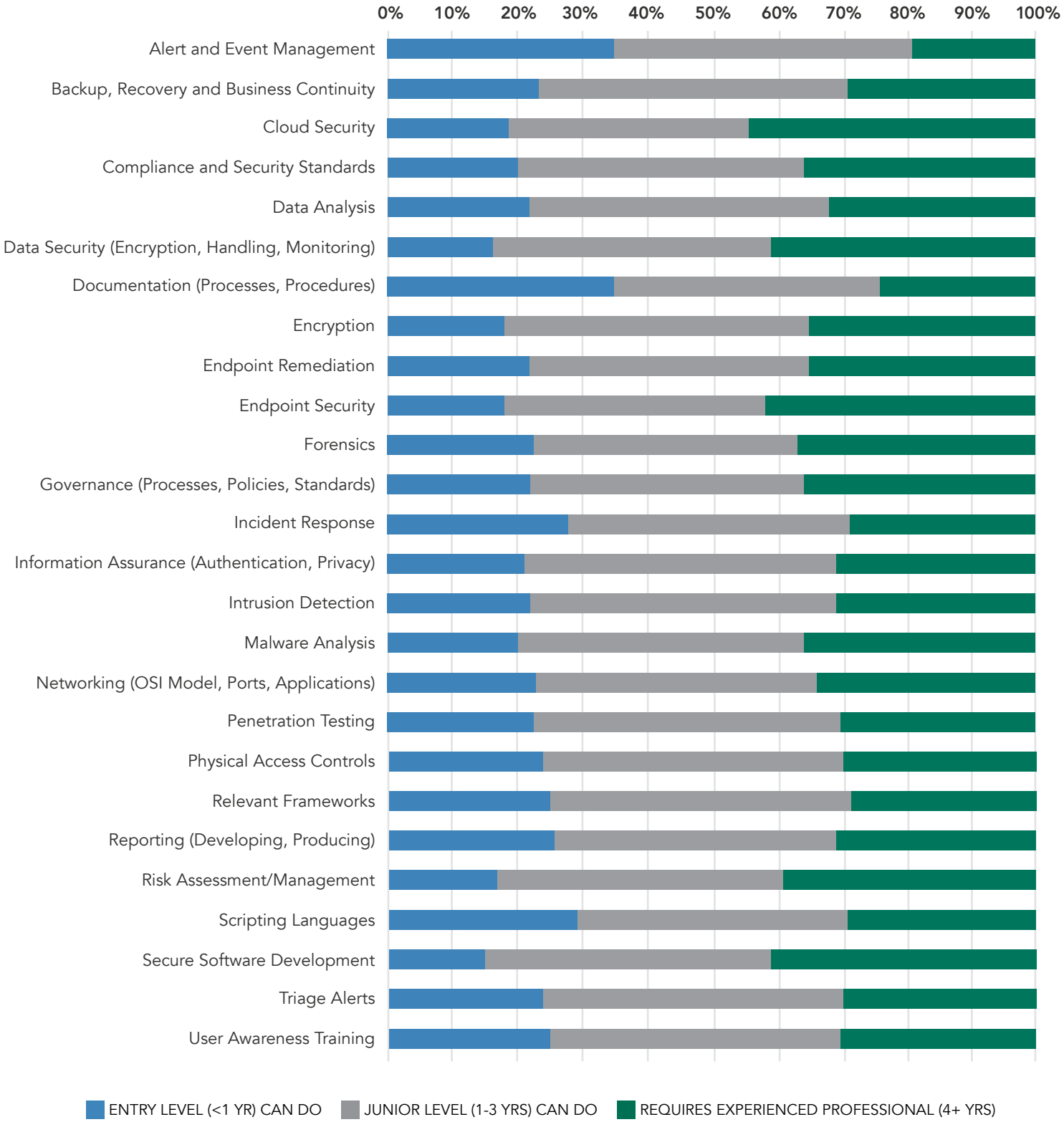
- **48%** Information Assurance (Authentication, Privacy)
- **48%** Backup, Recovery and Business Continuity
- **47%** Intrusion Detection
- **47%** Encryption
- **47%** Penetration Testing

Differences in task assignment across organizational size were also revealing. Hiring managers at organizations with 2,500 or more employees are more likely to assign cloud security responsibilities to their more experienced cybersecurity team members than their counterparts within small and midsize companies. However, nearly a quarter (23%) of managers at midsize companies (500 to 2,499 employees) believe entry-level staff are equipped to handle cloud security.

Small businesses and enterprise companies agree endpoint remediation should be handled by more experienced professionals. When it comes to forensics, the larger the organization, the greater number of managers feel that more experienced team members should handle the task. Meanwhile, 38% of managers at small organizations — those with fewer than 100 employees — believe entry-level team members can handle forensics.

Despite the variances, there are some general trends linking task assignment to experience.

Cybersecurity Task Assignments by Experience Level



We asked participants to tell us what tasks can be expected of staff at various years of experience, ranging from entry (less than one) to junior (one – three years) and experienced (greater than four years). Findings show that junior-level practitioners are equipped with the skillset to handle most cybersecurity tasks, freeing up experienced professionals' time to focus on more advanced tasks, such as secure software development, endpoint security, data security and risk assessment.

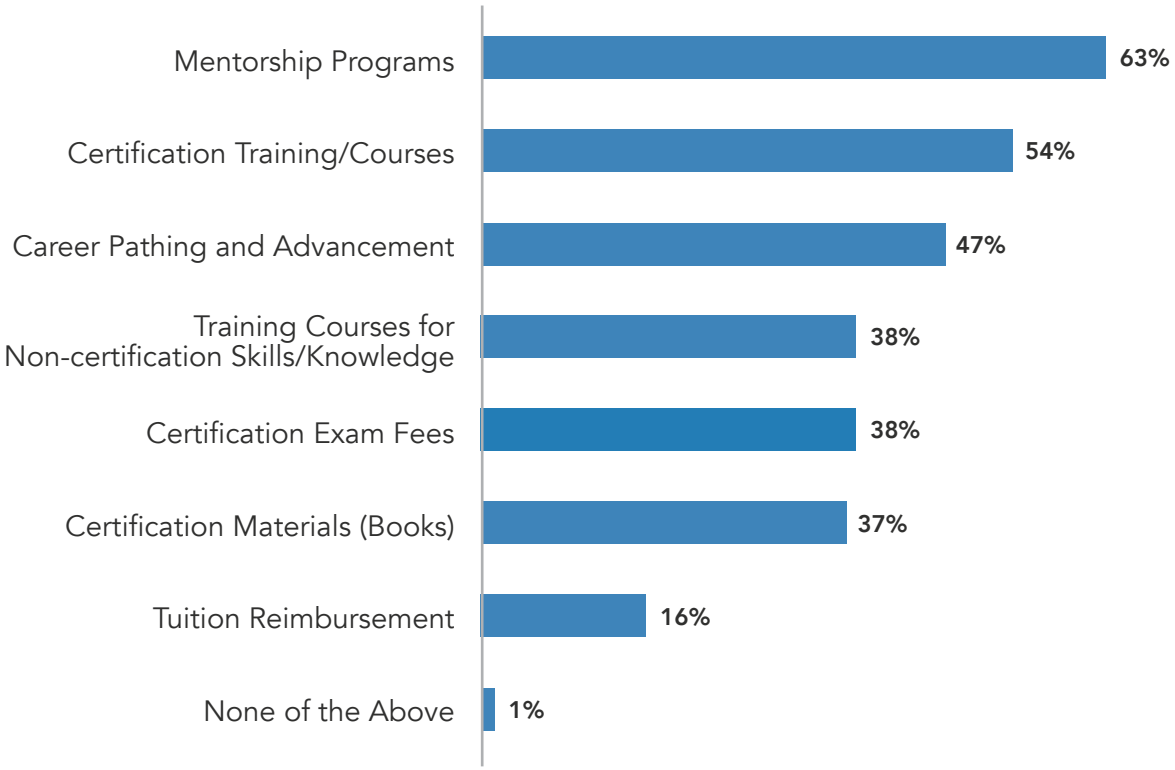
Investing in Professional Development

One of the most promising insights from our research is the revelation that participants value investing the time and money to train entry- and junior-level staff. They recognize the value in giving staffers time to develop, which ultimately leads to value back to their teams and organizations. Additionally, it provides a benchmark for other organizations and hiring managers to understand how long it can take for newcomers to be ready to operate independently and how much it typically costs.

91% of hiring managers say they allow entry- and junior-level cybersecurity team members career development time during work hours. The practice is only slightly less common in the U.S., where 87% of hiring managers offer it, compared to Canada (93%), the U.K. (94%) and India (93%).

As with hiring methods and task assignation, there is wide variation on how companies go about career development. Practices include mentorship programs, certification courses, career pathing and advancement, and non-certification-related training.

How Hiring Managers Develop Entry- and Junior-Level Staff



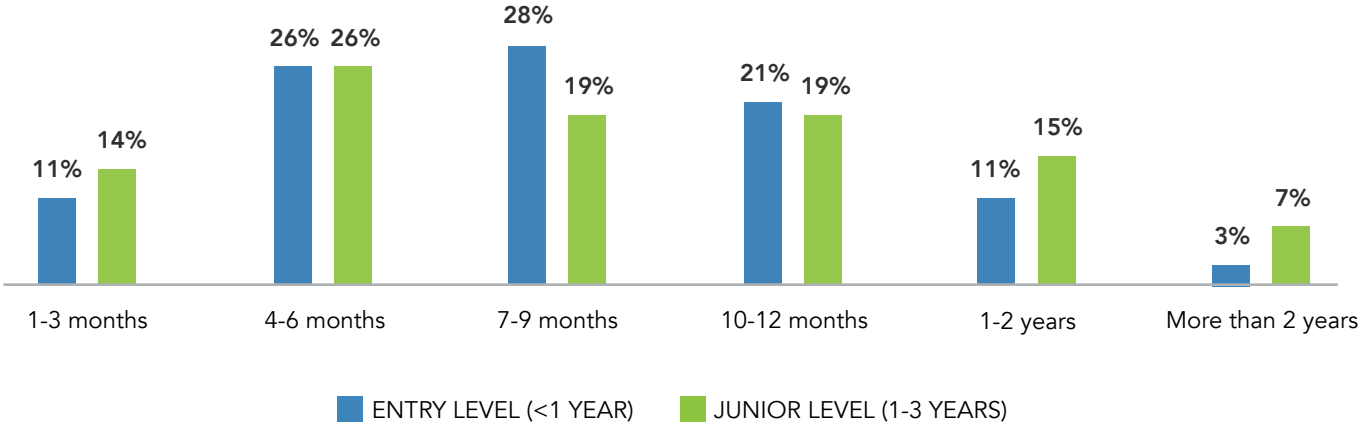
Mentorships, certifications and career pathing are among the tools and resources study participants offer to help newcomers gain experience, develop their skills and achieve new career milestones.

Midsize organizations lead the pack, offering professional development during business hours at the highest rates, while large organizations have the lowest rates. But larger organizations do more than the others with career pathing/advancement opportunities. This could be a result of having larger teams and, thus, more advancement possibilities. The practice of offering mentorships is more common in small companies, and it is the preferred method of professional development in India. In the U.K., there is a stronger focus on certifications.

Certifications were ranked the most effective method of talent development for entry- and junior-level practitioners (27%), followed by in-house training (20%), conferences (19%), external training (13%), and mentoring (11%). However, in-house training topped the list at smaller companies, while midsize organizations prefer conferences, and large companies favor webinars.

Time is certainly an investment required for developing entry- and junior-level cybersecurity practitioners. However, our study uncovered that it can take a relatively short amount of time before new entrants can handle assignments independently. 37% of participants estimate entry-level practitioners are considered "up to speed" after six months or less on the job. Half said it takes up to a year. Another 14% put the estimate at more than a year.

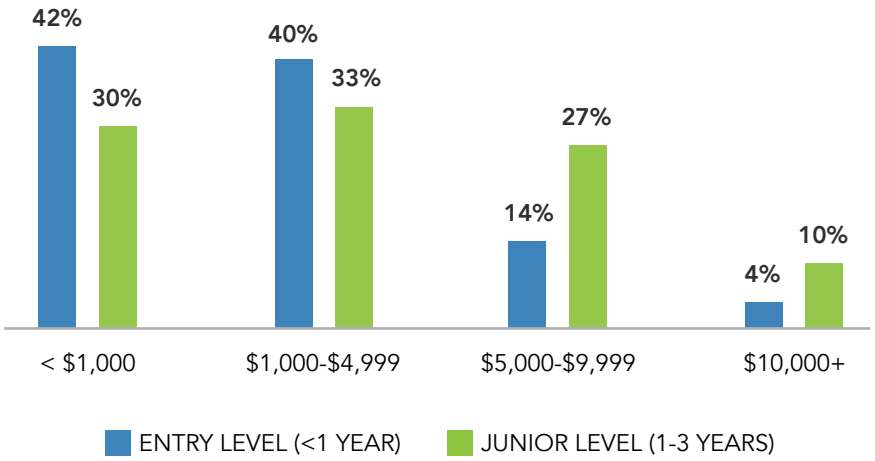
How Long Does it Take to Train Entry- and Junior-Level Staff?



65% of study participants say that entry-level staff are ready to work independently within nine months, with 37% saying it takes six months or less. These insights should be encouraging for any cybersecurity hiring managers concerned that training newcomers will take up too much time and resources.

Monetary investments in entry-level practitioner development are within reach of most organizations. 42% of participants said training costs less than $1,000 for entry-level hires to handle assignments independently, while 40% said it costs up to $4,999. Only 4% said the cost exceeds $10,000. 30% said it takes less than $1,000 for junior-level practitioners, 33% said up to $4,999, and 10% said more than $10,000.

How Much Will it Typically Cost to Train an Entry- or Junior-Level Staffer Before They are Able to Handle Assignments Independently?



Organizations do not need to allocate significant portions of their budget to the training and skill development of entry- and junior-level practitioners before they can handle tasks autonomously. 82% of participants say it costs less than $5,000 to train entry-level staff before they can handle assignments independently, with 42% saying it costs less than $1,000.

Benefit of Hiring at the Entry Level

The results of the study reaffirm the benefits organizations reap when they hire entry- and junior-level cybersecurity staff. When asked how these professionals have helped their organization, participants said they bring new perspectives, ideas, creativity, critical skills in new technologies, enthusiasm and reinvigorating energy.

One participant noted, "Having junior-level cybersecurity team members is very important in helping an organization grow. They bring new ideas to the table. The fact that they have less experience means that they are also more flexible to new ideas, and I think that is a very important factor to have in an ever-growing company and market."

How have entry- or junior-level cybersecurity team members helped your organization?

"They often bring an element of creativity and out-of-the-box thinking to the team."

Another said, "They can bring new ideas and break through the limitations of existing teams."

Additionally, said one participant, "They're often well versed on the newest innovations, even more so than some of our established senior contributors, while lacking skills to support their curiosity, and it creates excellent synergy."

Participants also noted that having entry- and junior-level practitioners on their cybersecurity team enables senior team members to focus on advanced work as "they take on a lot of the day-to-day work to free up senior people for more technical work." One participant noted that having entry- and junior-level team members on the team accelerates work, another noted they improve efficiencies.

CONCLUSION AND RECOMMENDATIONS

The (ISC)² Cybersecurity Hiring Managers Guide provides insights into how hiring managers and cybersecurity teams are recruiting and developing talent. When paired with insights from the (ISC)² Cybersecurity Careers Pursuers Study[6], hiring managers should have a better sense of realistic expectations for entry- and junior-level professionals and how to set them on the path to success.

Consider these five best practices when building your cybersecurity teams:

1. **Embrace Entry and Junior-Level Practitioners** – Hiring managers say their investment of time and resources has significant returns with the new energy, passion and perspectives they gain from recruiting entry- and junior-level team members.

2. **Look Beyond IT** – As the cybersecurity field draws younger and more diverse talent, hiring managers should carefully consider the non-technical skills and traits that indicate strong candidates for long-term career success.

3. **Partner with HR for Winning Job Descriptions** – Job descriptions should be a shared responsibility. Work closely with HR to create realistic job descriptions for entry- and junior-level roles that establish clear expectations for new hires and employers.

4. **Carefully Assign Tasks to Newcomers** – Consider the task and responsibilities respondents cited as appropriate for staffers at different experience levels. Assign duties to newcomers that enable them to learn and grow on the job, but also free senior team members to focus on high-priority assignments.

5. **Invest in Professional Development** – Best practices indicate that making time for learning during work hours, mentorship programs, certification attainment, training and clear career pathways are key to developing and retaining junior talent.

[6] The (ISC)² Cybersecurity Career Pursuers Study

Survey Methodology

We surveyed a total of 1,250 cybersecurity hiring managers from the United States (500), Canada (150), United Kingdom (200), and India (400). The survey was conducted in December 2021. To be eligible to participate, managers had to have hired entry or junior cybersecurity professionals in the past two years, managed a team with existing entry- or junior-level cybersecurity professionals; or be willing to hire entry- or junior-level professionals for their security teams. The margin of error for the global descriptive statistics in this research is +/- 2.8% at a 95% confidence level.

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 168,000 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.