MARKET RESEARCH

(ISC)² Cybersecurity Hiring Managers Guide

Asia-Pacific Edition

Trends and Insights for Hiring and Developing Entry- and Junior-Level Cybersecurity Professionals

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

TABLE OF CONTENTS

INTRODUCTION

One of the most often cited statistics from the COVID-19 pandemic is the unprecedented rate of digitalization across all industries and organization sizes.

This momentum is showing no sign of slowing. According to market research firm IDC, global digital transformation spending is forecast to hit a record high of U.S. $1.8 trillion in 2022, an increase of 17.6% over 2021.

In the midst of this digital gold rush, the role of cybersecurity has never been more important. Every new digital tool and employee added to an organization's arsenal can be compromised, creating a buffet spread of attack surfaces and vectors.

Threat actors are sitting up and taking notice. Not a week goes by without cyberattacks, data breaches, and the like hitting the airwaves. While major incidents affecting large global corporations dominate the headlines, small and midsize businesses with regional and local operations are equally if not more vulnerable.

Such is the backdrop against which cybersecurity professionals today operate. As organizations work to shore up their defenses, they continue to run into a common challenge: insufficient talent to join the ranks of their frontliners.

Hiring managers in the region have often looked towards entry- and junior-level candidates to fill vacancies. This report confirms the strategy continues. Additionally, the study explores how candidate sourcing, attributes and skills, and development practices are evolving.

The key takeaway is clear: all organizations in the industry have a role to play in expanding the cybersecurity talent pool across Asia-Pacific. Like the proverbial tide that raises all boats, it is only through everyone's involvement that we can create a safer and more secure digital world for all.

[1] IDC, 2022. Worldwide Digital Transformation Investments Forecast to Reach $1.8 Trillion in 2022, According to New IDC Spending Guide. Retrieved 11 September 2022 from https://www.idc.com/getdoc.jsp?containerId=prUS49114722

Research Methodology

This report seeks to better understand how hiring managers recruit and support the career development of entry- and junior-level cybersecurity practitioners.

Many organizations still find it a challenge to fill senior cybersecurity headcounts. A focus on understanding the hiring practices for early career professionals can help the industry create a foundational talent pool that leads to the easing of the talent bottleneck over the long term.

(ISC)² conducted a survey of 787 managers responsible for hiring and managing entry- and junior-level cybersecurity roles in four key Asia-Pacific countries: Hong Kong, Japan, Singapore and South Korea. The survey was fielded in June 2022.

For the purposes of this study, "entry-level" is defined as less than one year of experience, and "junior-level" refers to professionals with one to three years of experience.

Respondents came from a mix of industries (e.g., IT services, manufacturing, retail, etc.) and organization sizes, allowing the results to be generalized across the profession.

Most participants (79%) have hired an entry- or junior-level cybersecurity professional in the past two years. Those who had not directly hired in the past two years already had entry- or junior-level professionals on their teams.

Respondent Profile

NO. OF EMPLOYEES IN ORGANIZATION

44% Small (<500)

37% Mid Size (500-2,499)

20% Large (2,500+)

78%
Have hired any entry or junior pros in the past two years

21%
Already had entry or junior pros on their teams

EXPERIENCE

8
years on average managing Security Teams

TOP INDUSTRIES

IT Services

Manufacturing

Banking/Insurance /Finance

Retail

LEVELS THEY HIRE AND MANAGE

20% Entry

37% Junior

56% Mid-Advanced

27% Expert

PATHWAY INTO CYBERSECURITY

36% IT

29% From other field

26% Education

7% Self-taught

Part 1: In Search of Talent

Building a future-proof cybersecurity workforce begins with the search for talent. Across Asia-Pacific, most respondents (53%) rely on standard job postings to begin this journey.

Meanwhile, the popularity of partnering with staffing and recruitment firms for junior- and entry-level roles is much lower at only 39% of respondents.

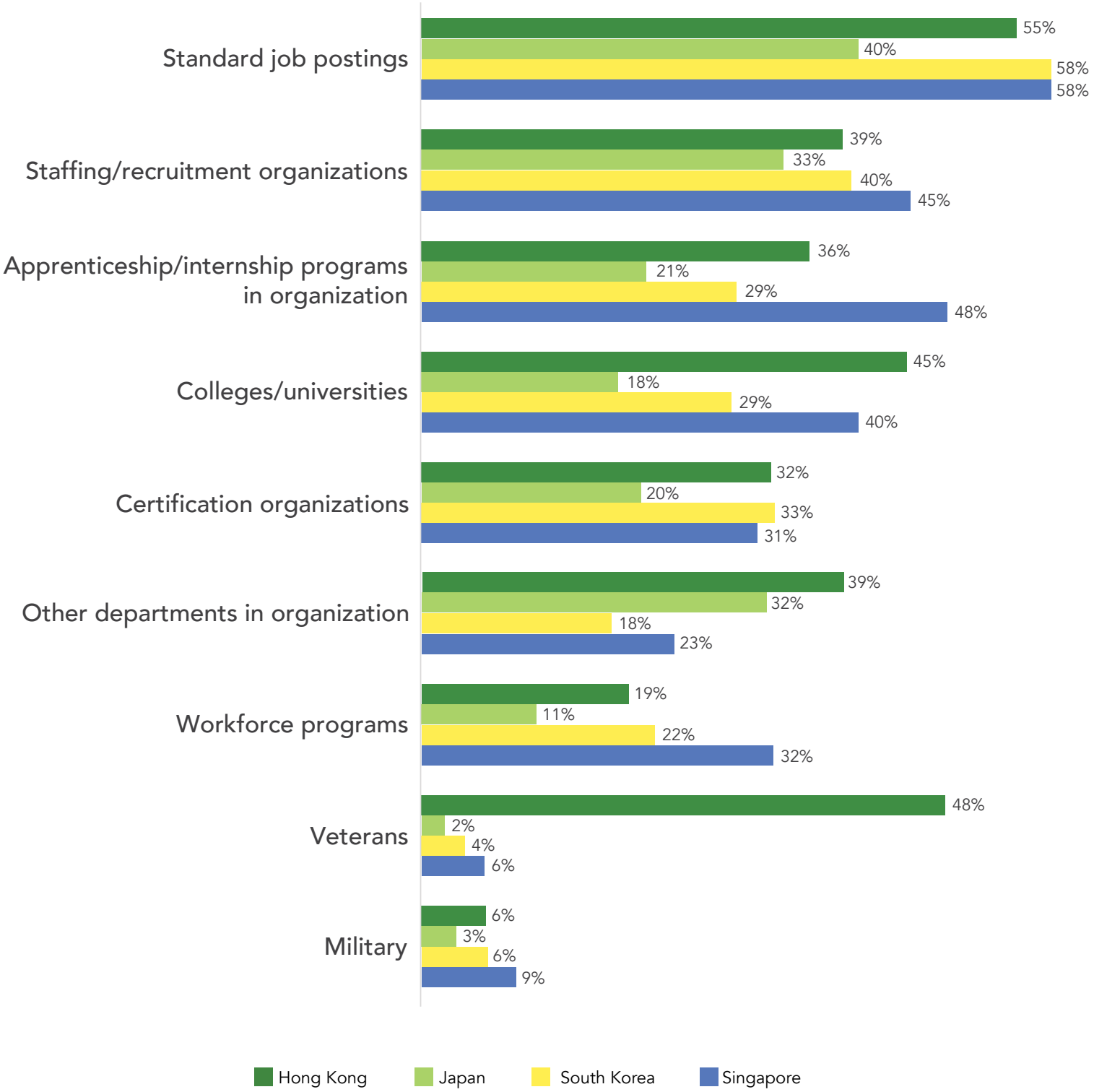
From which of the following have you identified or recruited entry- or junior-level cybersecurity candidates?

While most markets surveyed pointed to standard job postings as their top choice, differences have emerged at a local level.

For instance, 48% of Singapore respondents said they use apprenticeship or internship programs at their organizations to identify or recruit candidates, far surpassing the other markets surveyed.

Hong Kong participants showed a higher preference than other markets for hiring directly from colleges and universities (45%) as well as recruiting from other departments in their organizations (39%).

From which of the following have you identified or recruited entry- or junior-level cybersecurity candidates?



Building Job Descriptions

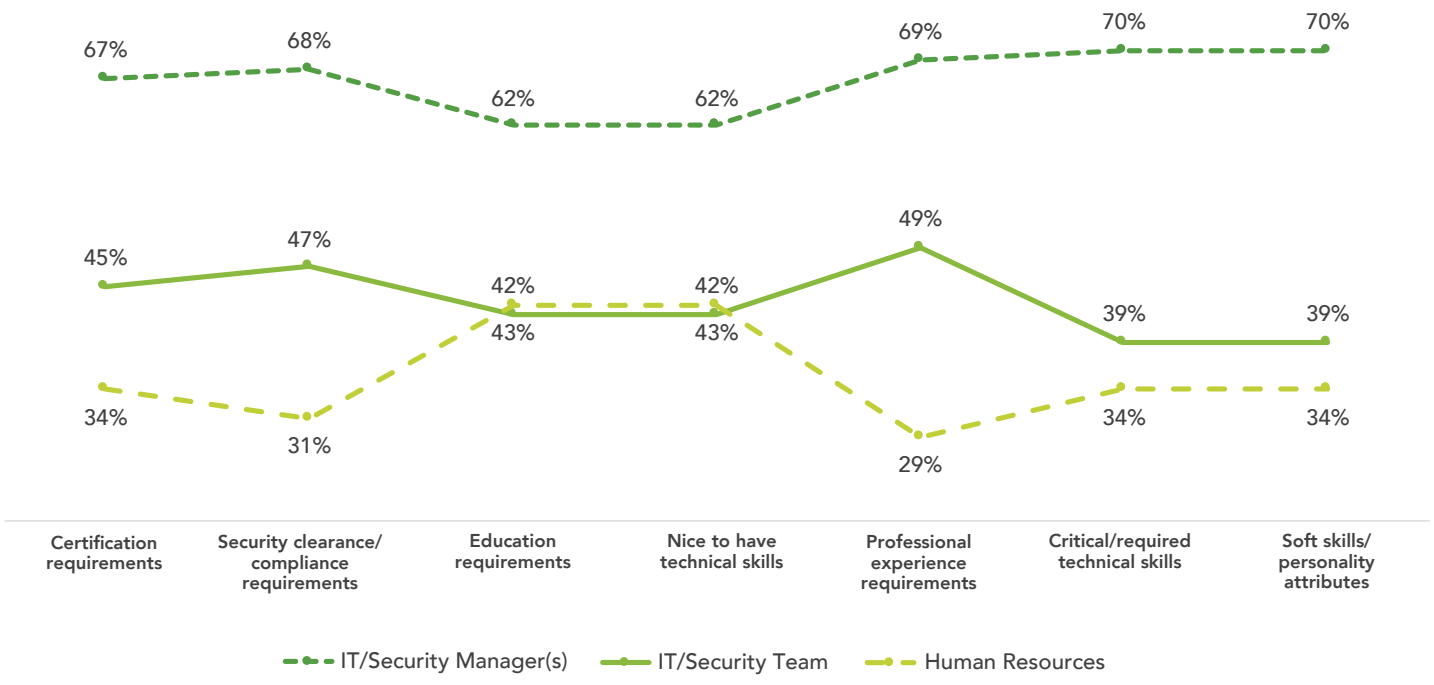
To hire the right candidates, organizations must first develop appropriate job descriptions for the roles they are hiring for.

This can be easier said than done. Job descriptions need to walk a tightrope between accurate depictions of what the job looks like on a day-to-day basis along with marketing more aspirational qualities to attract candidates of a more ambitious and growth-oriented caliber.

Our study revealed that while IT/security managers and their teams still take the lead in establishing the core requirements for creating a job description, HR departments are making their voices heard in two key areas: education requirements and nice-to-have technical skills.

This is noteworthy as it suggests that HR departments are playing a more active role in defining a broader range of what may be considered suitable qualifications for cybersecurity roles. This is beyond what IT and security managers may traditionally be on the look-out for.

Who determines the following requirements when creating a job description for an entry- or junior-level cybersecurity professional in your organization?



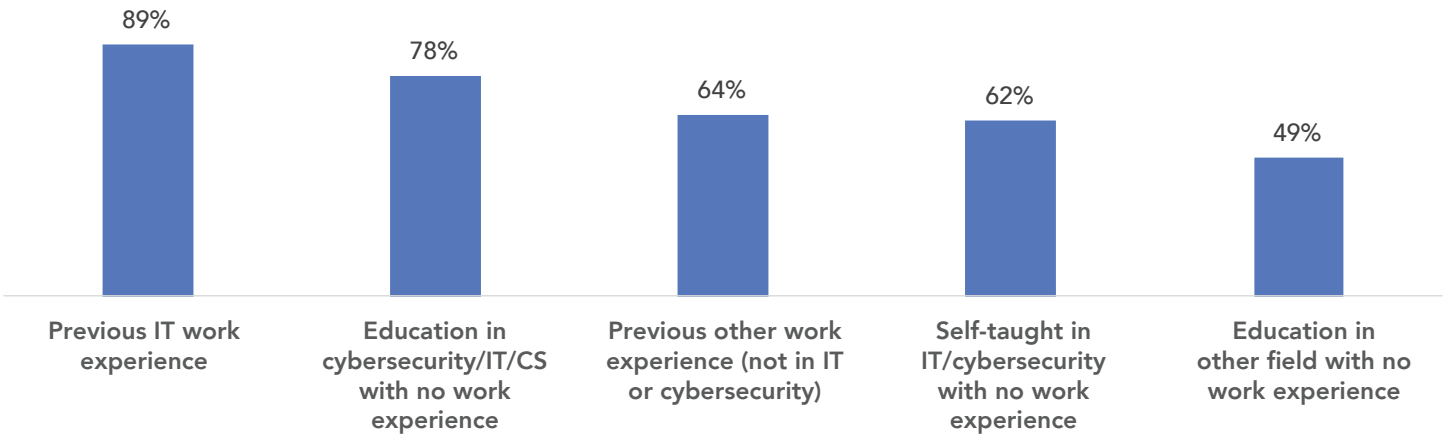
SPOTLIGHT: Looking beyond the IT talent pool

In general, hiring managers are increasingly sourcing for cybersecurity candidates from beyond the IT talent pool, both within and outside of their organizations.

Close to half of participants (49%) would consider a candidate with no work experience and an education in fields that are not computer science, IT and cybersecurity.

Encouragingly, 62% would hire a candidate self-taught in IT/cybersecurity despite having no work experience, while 64% would hire someone with previous work experience but not in IT or cybersecurity.

Would you consider a candidate for an entry- or junior-level cybersecurity role with only the following experience? % indication "Yes" shown

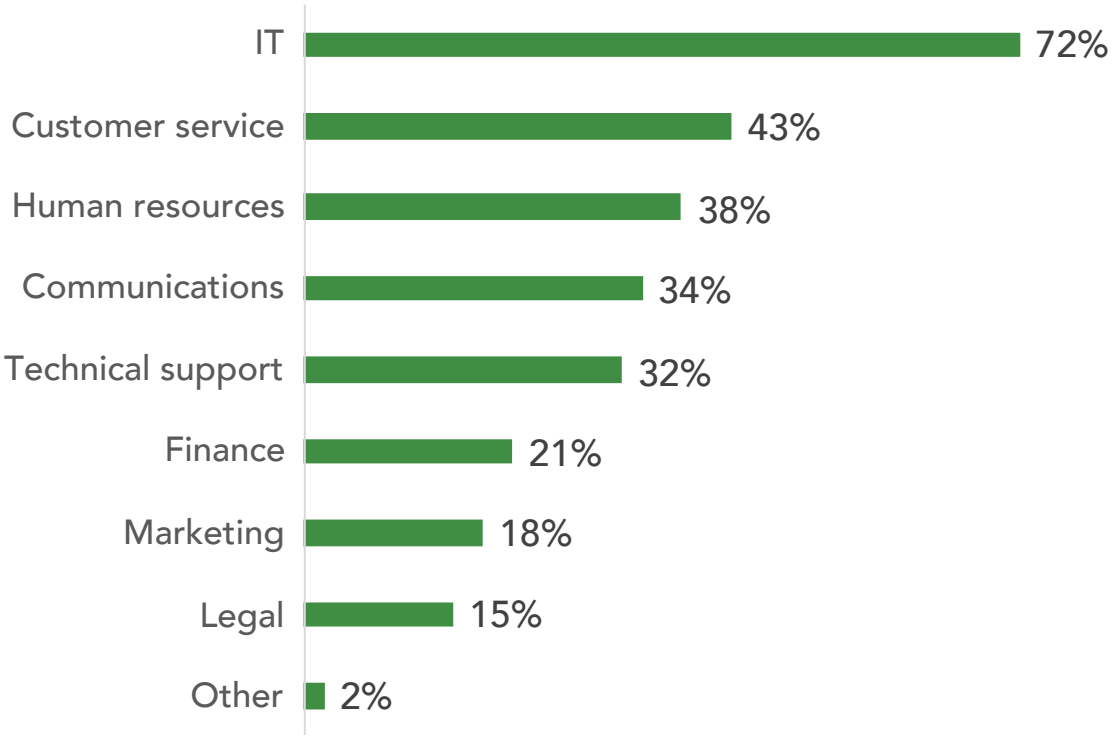


Local snapshot

- Respondents in Japan are the least likely to consider candidates with only education
- Those in Singapore and Hong Kong are most likely to consider self-taught candidates
- Singapore respondents are significantly more likely to consider candidates with education in a different field and no work experience

Within organizations, while IT departments continued to be the preferred source of talent by 72% of respondents for recruiting entry- or junior-level cybersecurity roles, hiring managers have also recruited from customer service (43%), human resources (38%), communications (34%) and even finance (21%) a and marketing (18%).

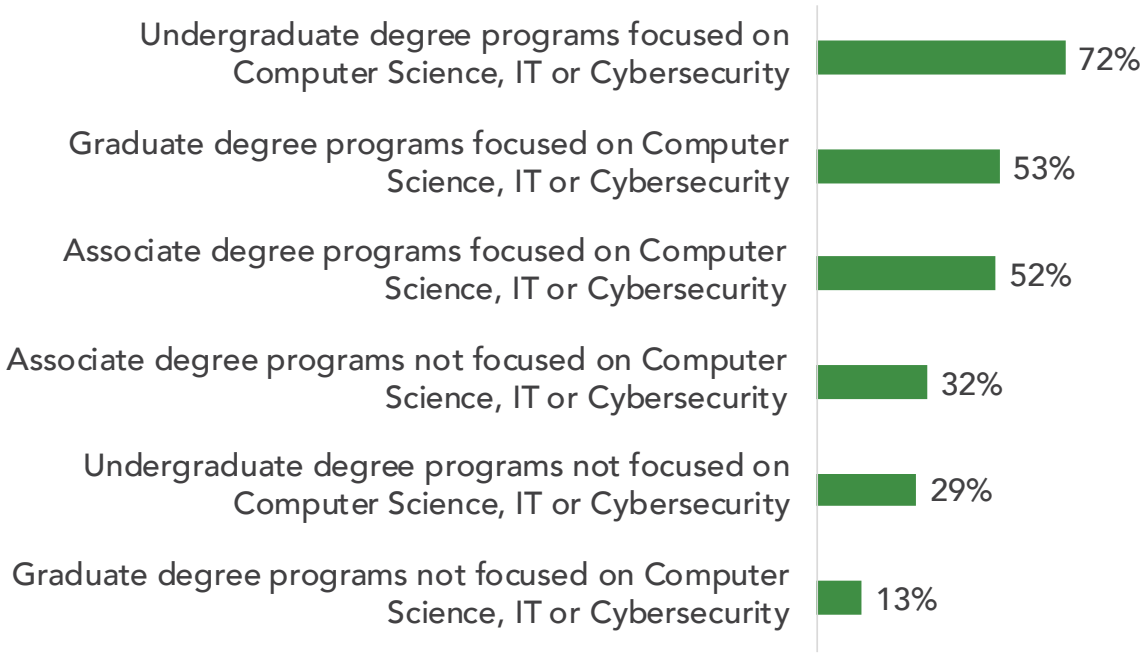
From which other departments within your organization have you recruited entry- or junior-level cybersecurity professionals?



In a similar vein, participants have also reported partnerships with educational programs beyond the traditional fields of computer science, IT and cybersecurity.

Although undergraduate and graduate degree programs focused on these subjects continue to form the bulk of partnerships (72% and 53% respectively), 32% of participants also said they have recruited from programs not focused on traditional fields, including associate (32%), undergraduate (29%) and graduate (13%) degrees.

From which of the following types of educational programs have you partnered with to identify entry- or junior-level cybersecurity candidates



Local snapshot

- Singapore and Japan respondents are more likely to partner with graduate degree programs
- Hong Kong respondents were significantly more likely to cite relevant associate degree programs than respondents from other countries
- Singapore respondents were most likely to partner with non-relevant associate degree programs

Part 2: Attributes and Skills

What are the top attributes and skills that hiring managers look for when hiring entry- and junior-level professionals?

Overall, 64% of hiring managers ranked previous professional experience as one of the most important attributes, followed by technical skills (56%) and certifications (51%).

In particular, the following local differences showed up in our study:

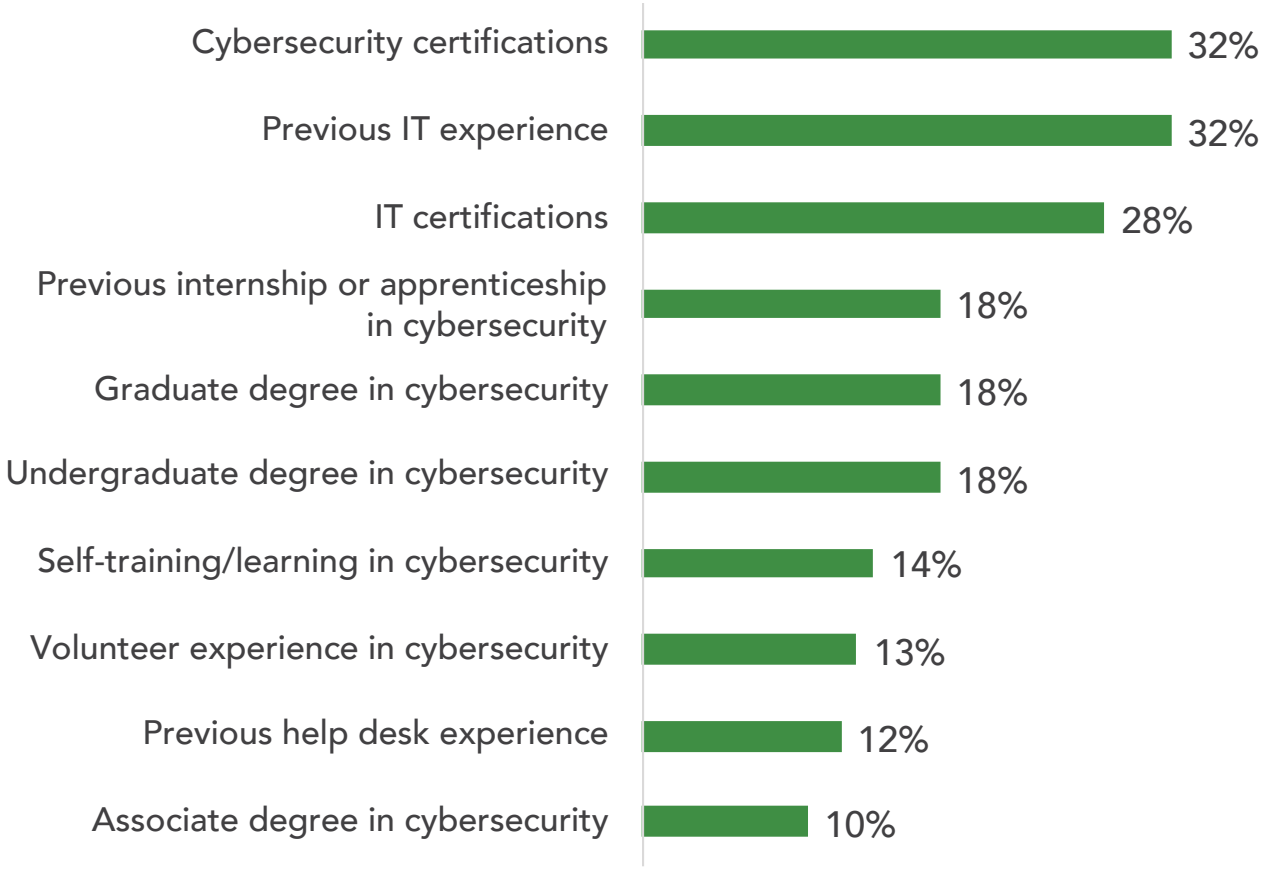
- Japanese respondents put a higher priority on previous experience vs. other countries. Conversely, certification was significantly less critical for Japanese respondents
- South Korea and Singapore ranked technical skills higher than Japan and Hong Kong
- Education was more important in South Korea and Hong Kong. IT experience was also significantly more critical for Korean respondents.
- Non-technical skills were least important in Singapore

Breakdown of Key Attributes

Unsurprisingly, when asked to rank which of these attributes are the post important, 32% of hiring managers said cybersecurity certifications are the most important attribute for entry- or junior-level candidates, tied with previous IT experience. IT certifications are also seen as highly important by 28% of respondents.

On the other hand, formal undergraduate and graduate degrees in cybersecurity did not rank among the top four most important attributes. This further reinforces the trend that recruiting from the general IT talent pool, as well as from candidates who have upgraded or proven their skills after graduation, are just as viable.

Of those items you rated as important for an entry- or junior-level cybersecurity candidate to possess, which two do you think are the most important?



Local snapshot

- Previous IT experience citation was significantly higher for Japan
- IT certifications were significantly more important to respondents in South Korea and Hong Kong
- Undergraduate degrees are more important among Hong Kong and Singapore respondents

Familiarity with Technical Concepts/Systems

Whether formally educated or self-taught, hiring managers expect candidates to display familiarity with technical concepts or systems, even if they belong to the entry- or junior-level career group.

Among these technical concepts or systems, participants were asked how they would rank the top five most important to them.

Naturally, broader concepts such as data security (34%) and security administration (32%) were ranked as the top two most important. This was followed by risk assessment/management (25%), backup, recovery, business continuity (24%) and compliance and security standards (24%).

More specialized areas like scripting languages and penetration testing ranked lower, but nonetheless scored in the double-digits.

Of the technical concepts or systems you rated as important for an entry- or junior-level cybersecurity candidate to understand, which five do you think are most important

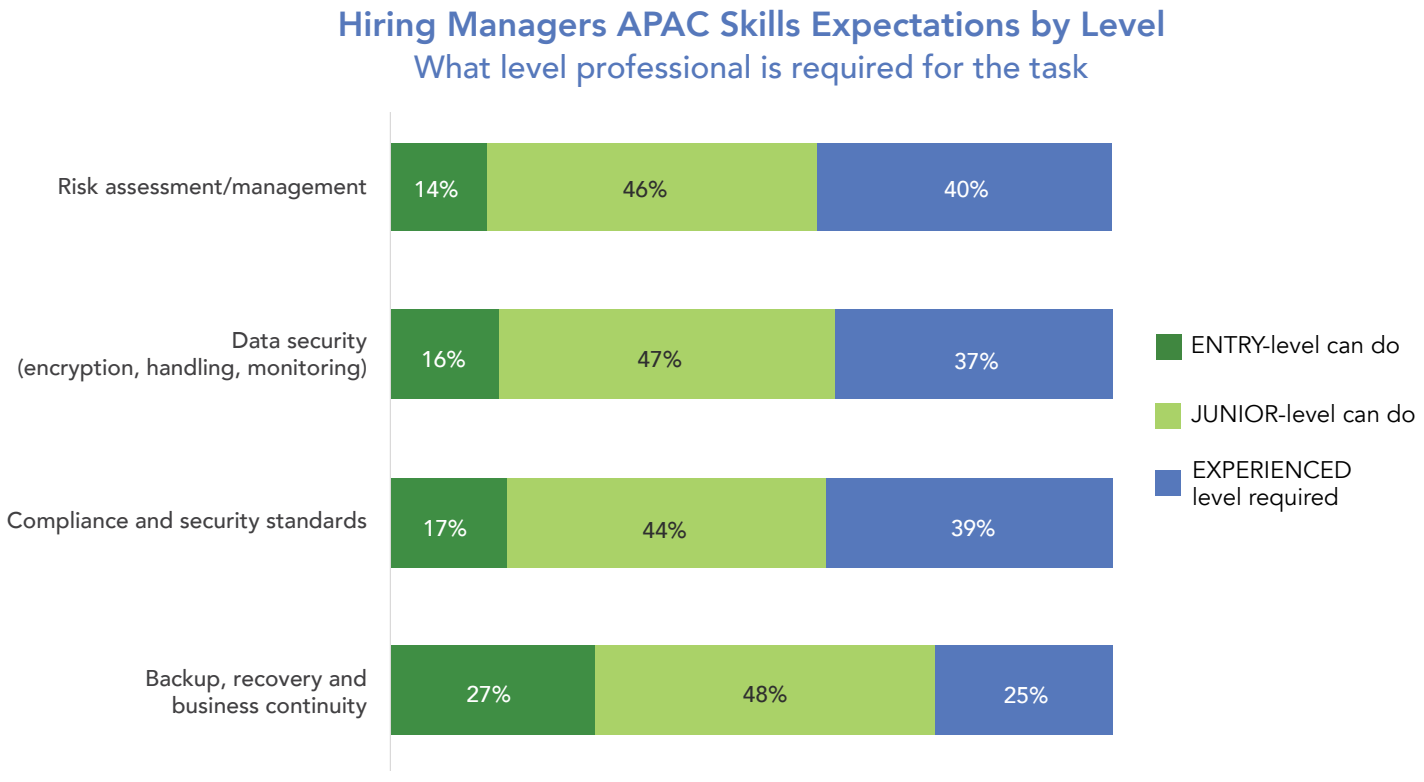
Local snapshot

- Data security is more important for respondents in Singapore and Hong Kong
- Security administration is less important for Singapore respondents
- Data analysis is significantly more important for Korean respondents
- Endpoint security is significantly more important for respondents at 5,000+ sized companies

It is important to note that how "technical familiarity" is defined will differ from one hiring manager to another. Is it therefore fair to expect entry- and junior-level employees to display the same level of expertise as a 10-year industry veteran?

However, most respondents agreed that entry- and junior-level employees should have no trouble accomplishing these tasks.

Here are the expectations of hiring managers around the top four concepts ranked earlier:



Even so, hiring managers understand that there are limits to each demographic's ability and experience, and adjust their expectations accordingly.

Top Tasks Entry-Level Can Do	%
Documentation (Processes, Procedures)	33%
Backup, Recovery and Business Continuity	27%
Scripting Languages	25%
User Awareness Training	23%
Physical Access Controls	22%
Alert and Event Management	22%
Reporting (Developing, Producing)	22%

Top Tasks Junior-Level Can Do	%
Alert and Event Management	57%
Triage Alerts	53%
Information Assurance (Authentication, Privacy)	53%
Relevant Frameworks	53%
Encryption	52%
Networking (OSI model, Ports, Applications)	51%
Reporting (Developing, Producing)	50%

Top Tasks Experienced Professional Required	%
Governance (Processes, Policies, Standards)	41%
Risk Assessment/Management	40%
Endpoint Remediation	39%
Forensics	39%
Secure Software Development	39%
Compliance and Security Standards	39%
Endpoint Security	37%

Non-technical Skills and Personality Attributes

While technical skills are important, hiring managers have also highlighted the importance of more well-rounded professionals who have also honed their non-technical skills, such as problem solving and teamwork.

In a stark juxtaposition, hiring managers expect candidates to work effectively both in a team, and on an individual basis – both of which emerged as two of the most highly rated non-technical skills.

Project management experience (27%), verbal communication (23%) and written communication (18%) rounded up the top five non-technical skills marked as the most important by respondents.

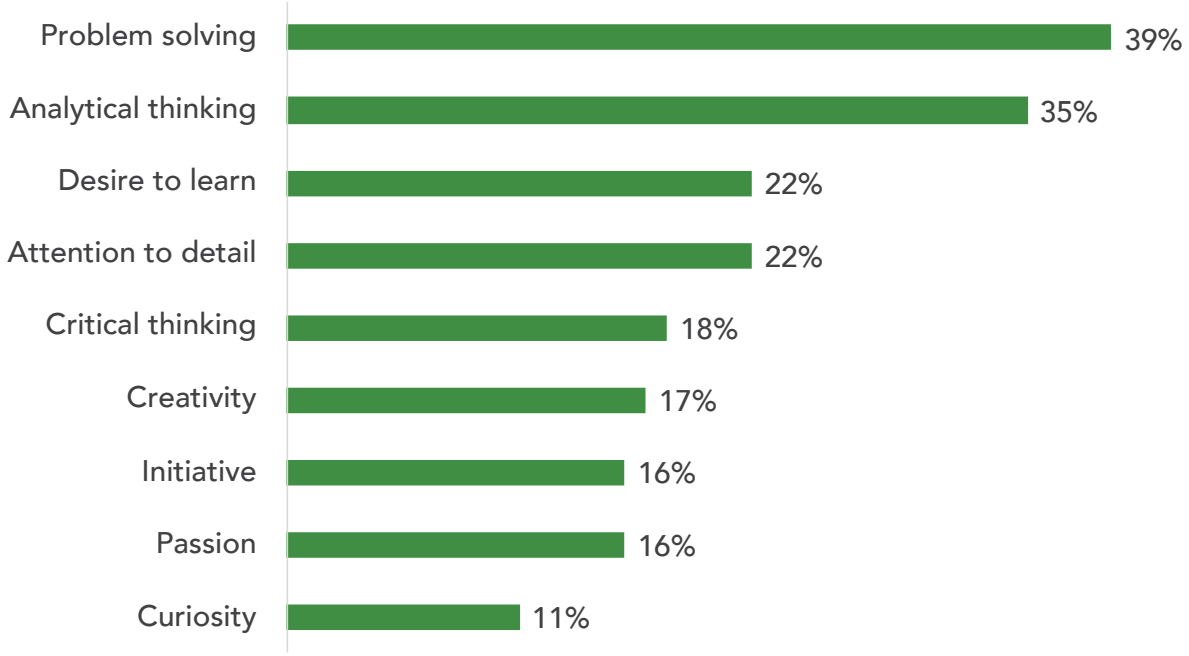
Of the non-technical skills you rated as important for an entry- or junior-level cybersecurity candidate to possess, which two do you think are most important

Interestingly, the ability to work independently was cited more frequently by respondents in Singapore and Hong Kong, though teamwork was still more important. Verbal and written communication was significantly more important for Japan when compared to other countries.

Personality-wise, our study found that hiring managers think it's important for candidates to display problem solving and analytical thinking traits.

A desire to learn was also called out as an important attribute, especially for a career like cybersecurity – and IT in general – where what we know today could be obsolete tomorrow.

Of the personality attributes you rated as important for an entry- or junior-level cybersecurity candidate to possess, which two do you think are most important?



Local snapshot

- Desire to learn and critical thinking was cited more frequently by Hong Kong and Singapore respondents
- Creativity was cited at a higher frequency among Korean respondents
- Initiative was more popular among respondents in Singapore and Japan
- Attention to detail was cited more frequently by organizations with 5,000+ employees

Part 3: Professional Development

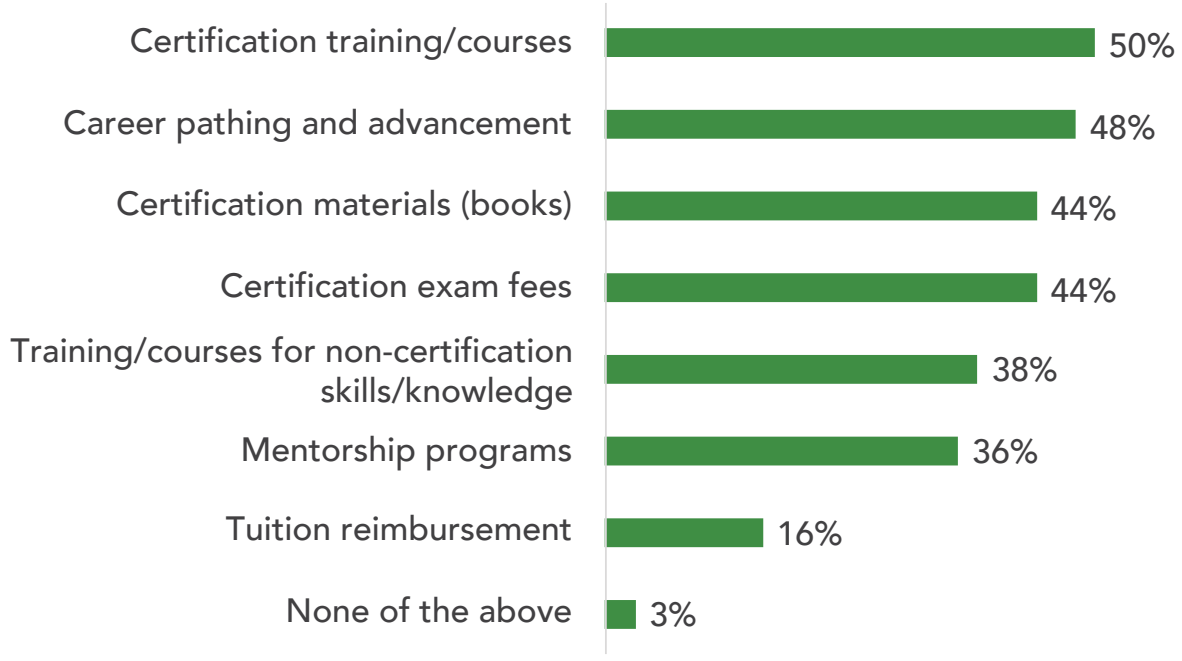
Indeed, given the constantly evolving nature of cyber threats, and the unceasing development of new technology and best practices for dealing with them, a desire to learn could perhaps be one of the most important signals for successful cybersecurity professionals over their long-term careers.

There is visible evidence of a demand by cybersecurity practitioners to upgrade their skills and keep them current as they progress through their career. Hiring managers surveyed for this study recognize this, with the vast majority (97%) stating that they provide some form of professional development for their entry- and junior-level staff.

Certification training and courses top the list at 50%, a point also supported by the provision of certification materials such as books (44%) and the sponsorship of certification exam fees (44%).

A variety of other professional development opportunities complete the list, including mentorship programs and non-certification training.

Which of the following does your organization provide to your entry- or junior-level professionals?



Cultural differences are also reflected in our study participants' approach to training and professional development.

- Japan is significantly less likely to offer certification training and career pathing, according to respondents
- The sponsorship of certification exam fees was cited at a significantly higher rate among respondents in Hong Kong
- In Singapore, respondents are significantly more likely to offer training for non-certification skills and mentorship programs than other countries

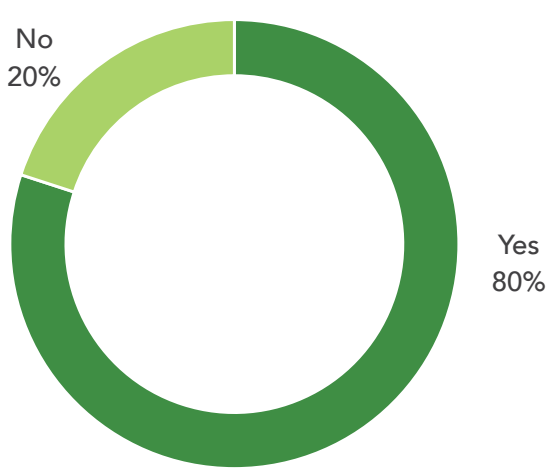
In an age where learning takes many forms, most organizations recognize that professional development can take place at anytime and anywhere.

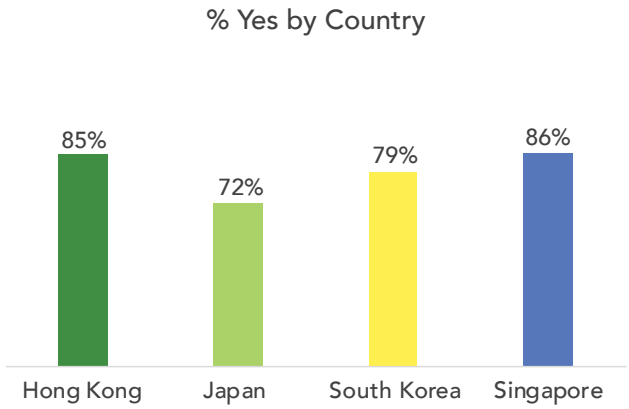
Some 80% of respondents reported that they allow entry- or junior-level employees to engage in professional development activities during work hours, a substantial commitment from organizations across Asia-Pacific.

While this is a commitment to in-work training and development that can be applauded, it should be noted that this does not occur evenly across the markets studied.

In Japan, respondents confirming access to professional development time during working hours clocked in at 72% – lower than Singapore and Hong Kong, both of which stand at an impressive 85% or higher.

Do you allow entry- or junior-level cybersecurity professionals time for professional development during work hours?





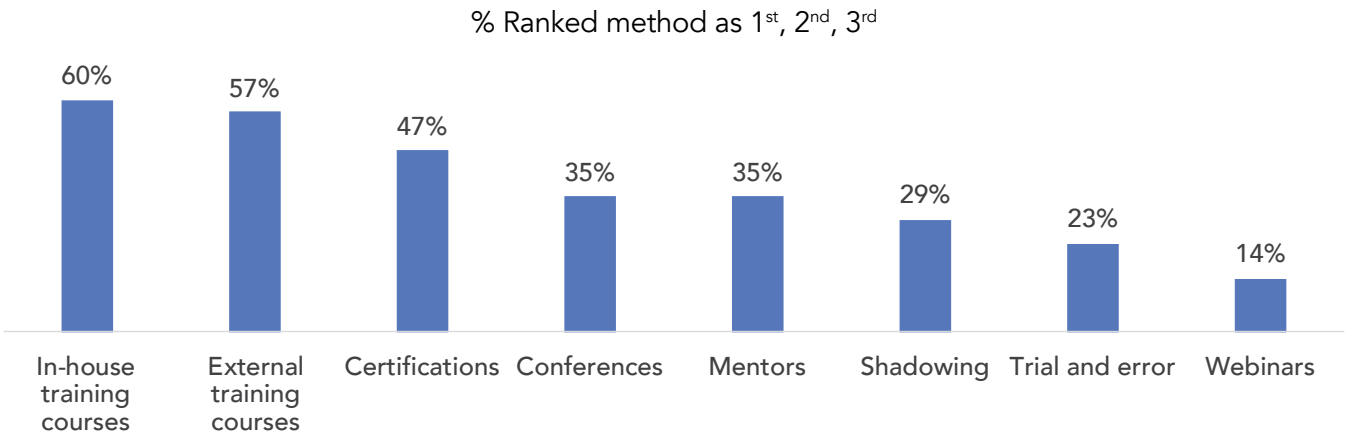
It is also worth noting that 20% of respondents overall said their organizations do not provide such an opportunity for entry- or junior-level staff – a gap that needs to be closed as soon as possible.

With such a wide variety of training options, the study polled respondents on which methods they think are the most effective.

Understandably, in-house training courses were rated by 60% as one of the most effective ways. This may be because organizations best understand their own business needs and can tailor in-house training materials accordingly.

Respondents also rated external training courses and certifications as highly effective training methods.

What is the most effective way to train entry- or junior-level cybersecurity professionals



Local snapshot

- In-house training was ranked highest by Hong Kong respondents
- Hong Kong and Japan ranked external training courses higher than Singapore and South Korea
- Conferences ranked higher among Korean respondents vs. others
- Shadowing is more popular in Singapore and Japan

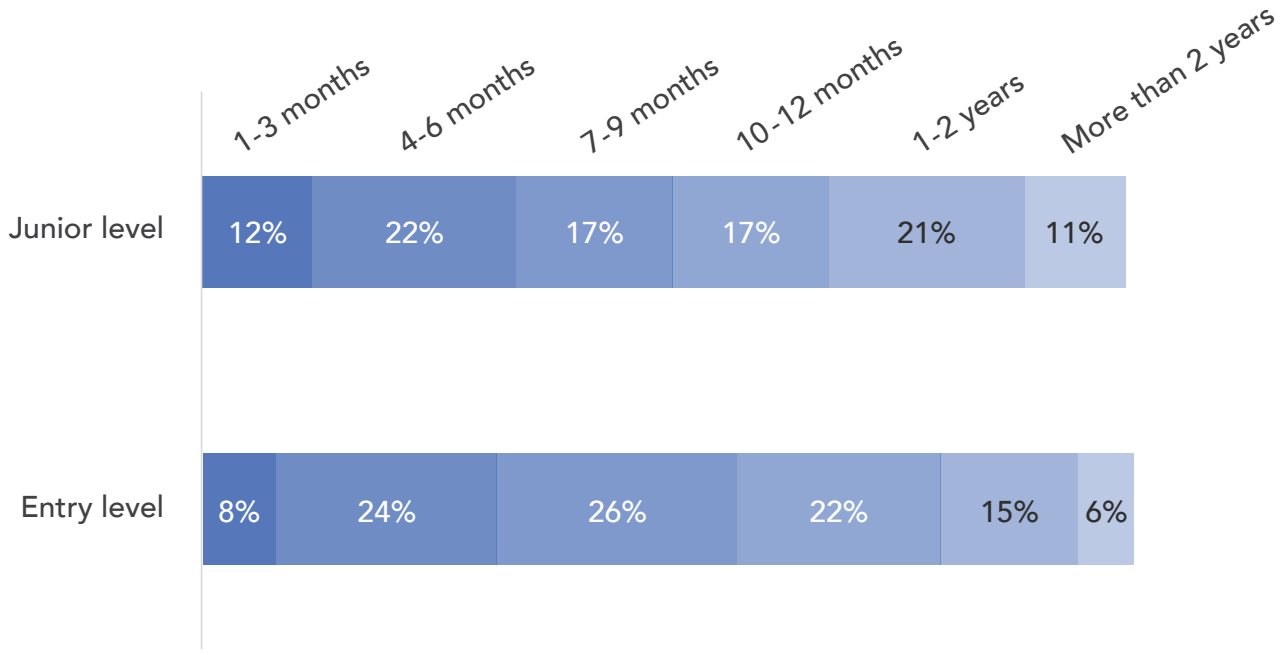
Investing in Professional Development

Whether formally educated or self-taught, hiring with clear demand for professional development, organizations might be wondering just how much to invest in the endeavor. This is not only measured in money; time is also a crucial factor, as every minute an employee spends on training means a minute away from their day-to-day job functions.

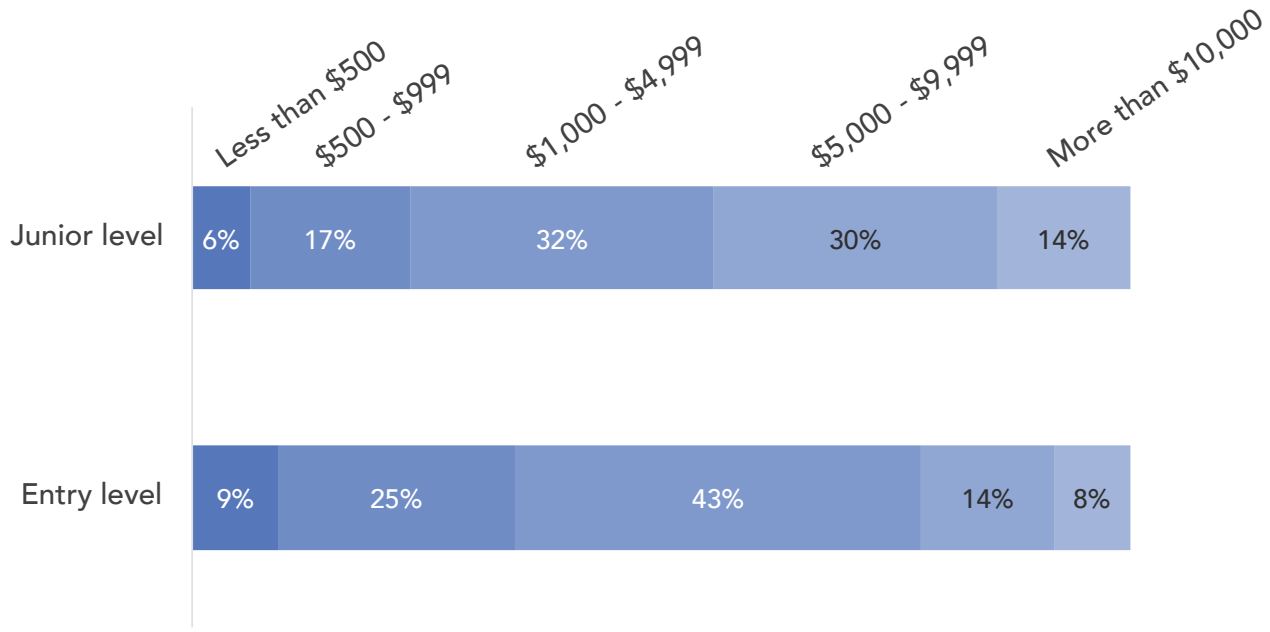
The hiring managers surveyed believe that most entry- and junior-level employees can be trained to handle assignments independently without supervision or guidance in under nine months. Only a small percentage report a training time frame of more than two years.

The majority of respondents also estimated that it will typically cost the equivalent of U.S. $1,000 to U.S. $4,999 to sufficiently train up both entry- and junior-level cybersecurity professionals to the point of competency without supervision.

How long does it typically take for an entry- or junior-level cybersecurity professional to be able to handle assignments independently (without supervision/guidance)?



How much will it typically cost to train an entry- or junior-level cybersecurity professional before they are able to handle assignments independently (without supervision/guidance)



Local snapshot

- Respondents in Singapore were nearly twice as likely to cite U.S. $1,000-U.S. $1,499 for entry level, and 1.5 times more likely for junior level
- Respondents in Hong Kong were twice as likely to cite more than U.S. $10,000 for entry level, and 1.5 times more likely for junior level

CONCLUSION

The Asia-Pacific cybersecurity workforce continues to face staffing challenges across the board. Notably, most of the findings from the study behind this Hiring Managers Report had no significant disparity between organization sizes.

This is a clear signal that the talent shortage in cybersecurity affects everyone. By uncovering the hiring and talent development strategies that organizations are adopting in responce to this talent shortage, (ISC)² has outlined the key trends and insights obtained directly from cybersecurity hiring managers themselves.

In particular, we expect the hiring of entry- and junior-level positions to truly take off from 2023, given its growing momentum so far.

Organizations can leverage the key takeaways and recommendations of this report to begin laying the groundwork for welcoming these new talents into their ranks, making sure the right hiring policies and professional development frameworks are in place.

TOP THREE TAKEAWAYS AND RECOMMENDATIONS

1. **Entry- and Junior-Level Hires Are Key to Closing the Talent Gap** – More than ever, hiring managers are recruiting entry- and junior-level roles to bridge the talent gap, alongside investing time and resources to grow their careers. Organizations who have not already done so risk falling even further behind in their search for talent.

2. **Listen and Look Beyond IT** – The cybersecurity field is growing dynamically, attracting talent from all over. Hiring managers should carefully consider the non-technical skills and traits that indicate strong candidates for long-term career success, broadening their search to include candidates that come with the right attributes, instead of only focusing on technical skills or past IT/cybersecurity experience.

3. **Professional Development Reaps Returns** – Entry- and junior-level recruits, as well as career switchers, might come with the right energy, attributes and attitudes, but they still need to be trained and supported so they can do their best work. To develop and retain these talents, organizations need to make time for their employees to learn during work hours, and provide opportunities like mentorship programs, certification attainment, as well as training and clear career pathways.

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 association of candidates, associates and members, nearly 280,000 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.(ISC)².org, follow us on Twitter or connect with us on Facebook and LinkedIn.

© 2022 (ISC)² Inc., (ISC)², CISSP, SSCP, CCSP, CAP, CSSLP, HCISPP, CISSP-ISSAP, CISSP-ISSEP, CISSP-ISSMP and CBK are registered marks, and CC is a service mark of (ISC)², Inc.