Hiring and Retaining Top Cybersecurity Talent

What employers need to know about cybersecurity jobseekers in 2018

(ISC)²®

INSPIRING A SAFE AND SECURE CYBER WORLD

INTRODUCTION

Many cybersecurity workers are open to new employment opportunities in 2018, according to new research by (ISC)^2, the world's largest membership association of certified cybersecurity professionals. On the flipside, employers may be in for a struggle as they seek to fill cybersecurity vacancies and retain workers, many of whom say they are spoiled for choice when deciding to switch jobs. In all, some 84% of cybersecurity workers are open to new employment opportunities in 2018, including 14% who are actively looking for a change.

Only 15% of cybersecurity professionals have "no plans" to leave their current employment, the study revealed. This group comprises mostly mid-career professionals who are content with their pay and work in smaller organizations where their opinions are heard. That the group is so small is problematic for employers. Most currently employed cybersecurity professionals (70%) are open to a change despite having no plans to begin a job search in 2018 – willing to be swept away by a recruiter.

This creates retention challenges, but it also opens opportunities for employers who adopt best practices in more accurately positioning roles and responsibilities when hiring cybersecurity professionals, as well as ensuring this talented workfroce remains satisfied. 68% want assurance the C-suite will take their opinions seriously about how to protect the organization. 62% want to work for an company with well-defined ownership of cybersecurity responsibilities. 59% view employee cybersecurity training and investments in emerging security technology as priorities.

Other positive organizational qualities that ranked high with study participants were the ability to "protect people and data" (62%) and "a strong code of ethics" (59%). Recruiters should take these to heart and resist the temptation to overemphasize pay, which is less of a priority. Thanks to high demand for talent, candidates likely view an attractive pay package as a given.

They want to work where security needs are taken seriously and where they can be the most useful in protecting an organization. More than half (54%) would work where a breach already has occurred, but they want to be forewarned of what they are stepping into. So employers need to be upfront with candidates, demonstrating they understand what cybersecurity workers value and painting an accurate picture of the organization's cybersecurity situation. Getting this right will help attract qualified candidates.

68% want their opinions taken seriously

62% prefer clearly defined cybersecurity responsibilities

59% prioritize employee training and tech investment

IN HIGH DEMAND

Any employer that has tried to recruit cybersecurity talent in the recent past knows how big a challenge it is. The competition is fierce. The research shows nearly half (46%) of cybersecurity professionals are contacted weekly by recruiters, regardless of whether they are actively looking for a job. 18% of cybersecurity professionals not seeking a new job receive calls daily from recruiters.

For some cybersecurity professionals, contact from recruiters is a daily occurrence, with one out of five (21%) study participants saying they receive at least one recruiting contact daily. And 38% of those actively seeking new employment are contacted multiple times each day.

While that much wooing from recruiters bodes well for jobseekers looking for new opportunity, employers need to be aware of the potential churn recruiters are encouraging with all their outreach.

Survey data also reveals a trend that entry-level and first-year employees aren't looking to change jobs. Although the study shows that beginning in year two the willingness to make a move starts to grow. This suggests their experience during that first year is critical to retention. As soon as a new cybersecurity job candidate gets their employee badge, employers have to start delivering on promises made during the recruitment process. Those promises should include a willingness to listen to cybersecurity employees' views and establishing clearly defined job responsibilities.

Figure 1 – How Often Cybersecurity Professionals are Contacted by Recruiters

Active jobseekers are contacted quite frequently, with 31% reporting they are contacted once a week; 19% say a few times a week; and 6% say recruiters find them daily. Employers should note, however, that as many as 18% of cybersecurity professionals not seeking a new job receive calls daily from recruiters, emphasizing again how competitive the cybersecurity talent market is.

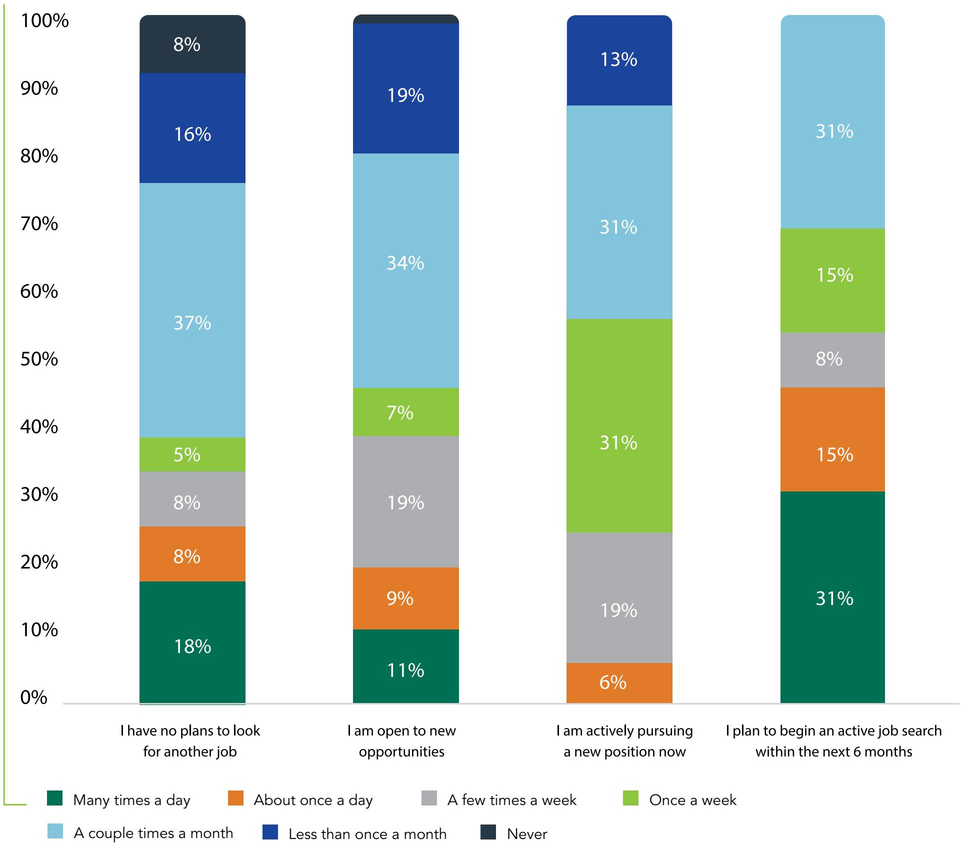
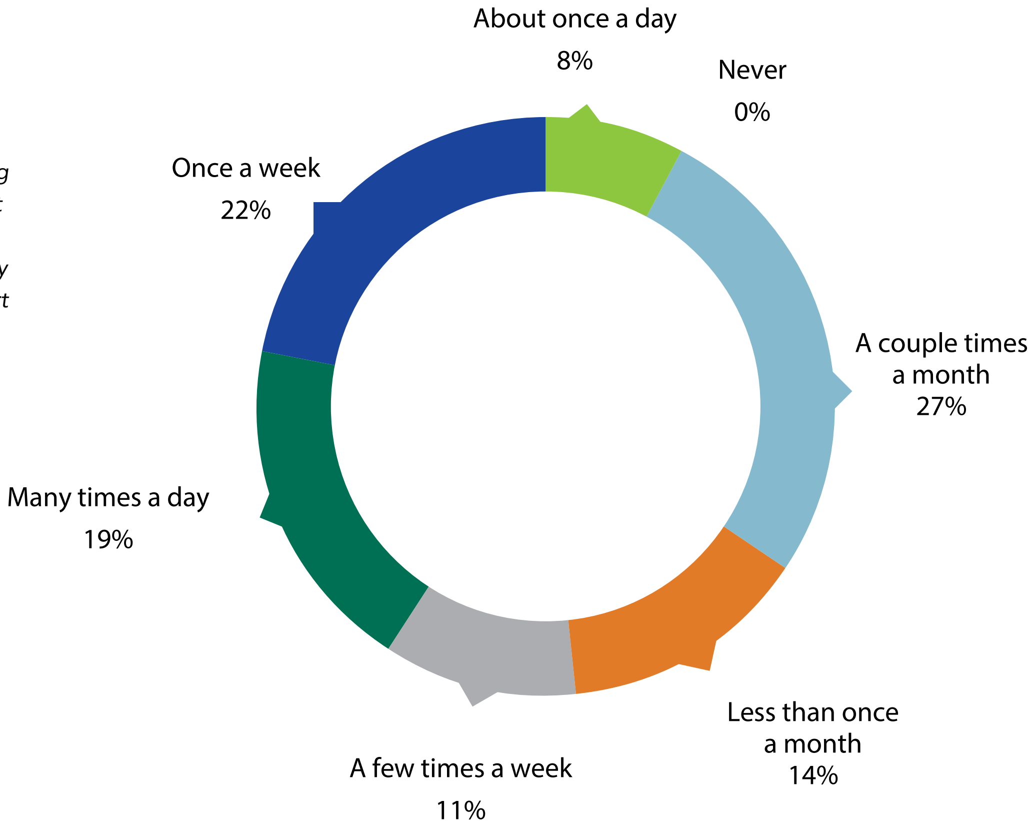


Figure 2 – Recruiter Contact Frequency for Cybersecurity Professionals Looking for a New Job in 2018

Nearly 20% of cybersecurity professionals already pursuing a new job or planning to start their job search in 2018 are contacted multiple times daily by recruiters. Only 14% report receiving calls from recruiters less than once a month.

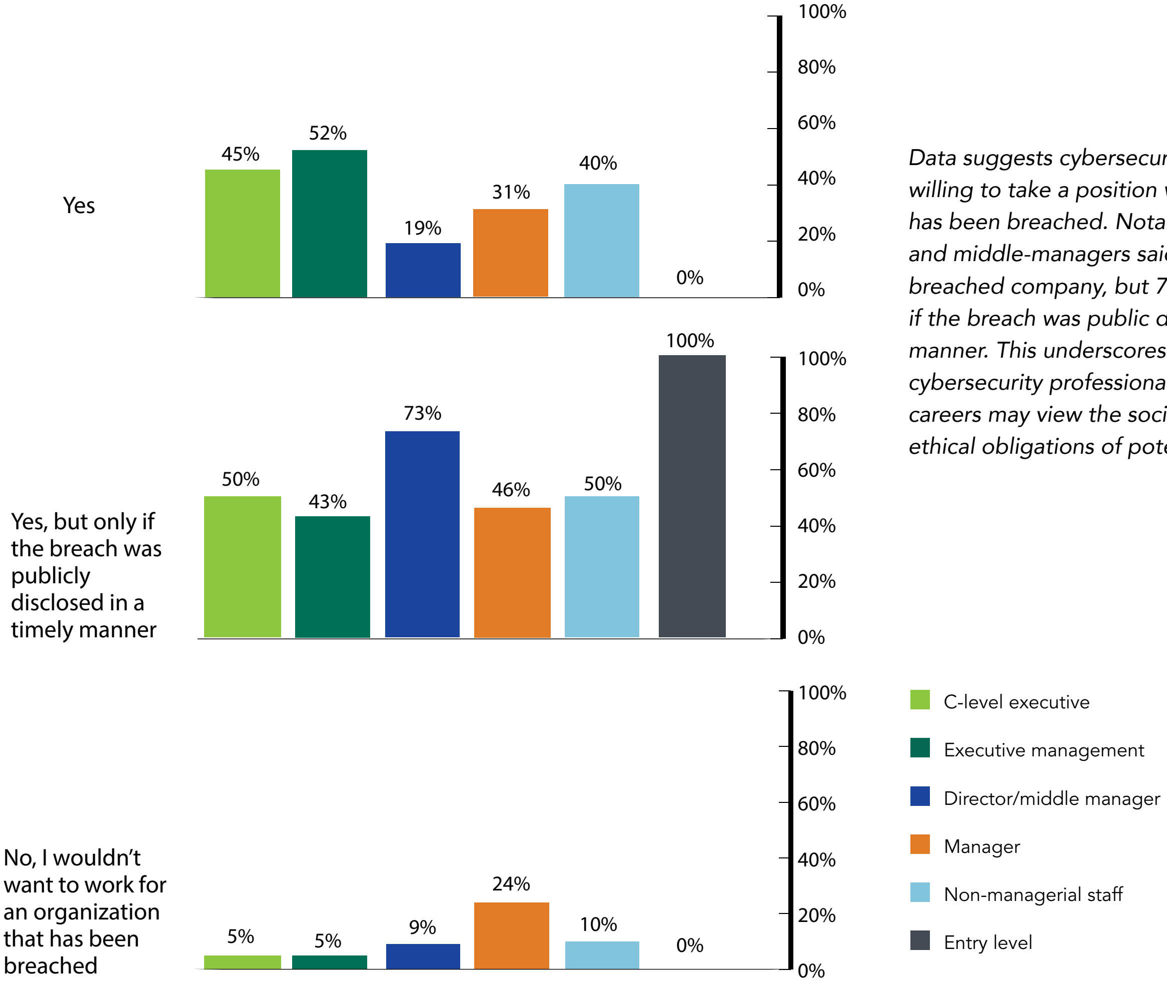


JOBSEEKER CAUTION

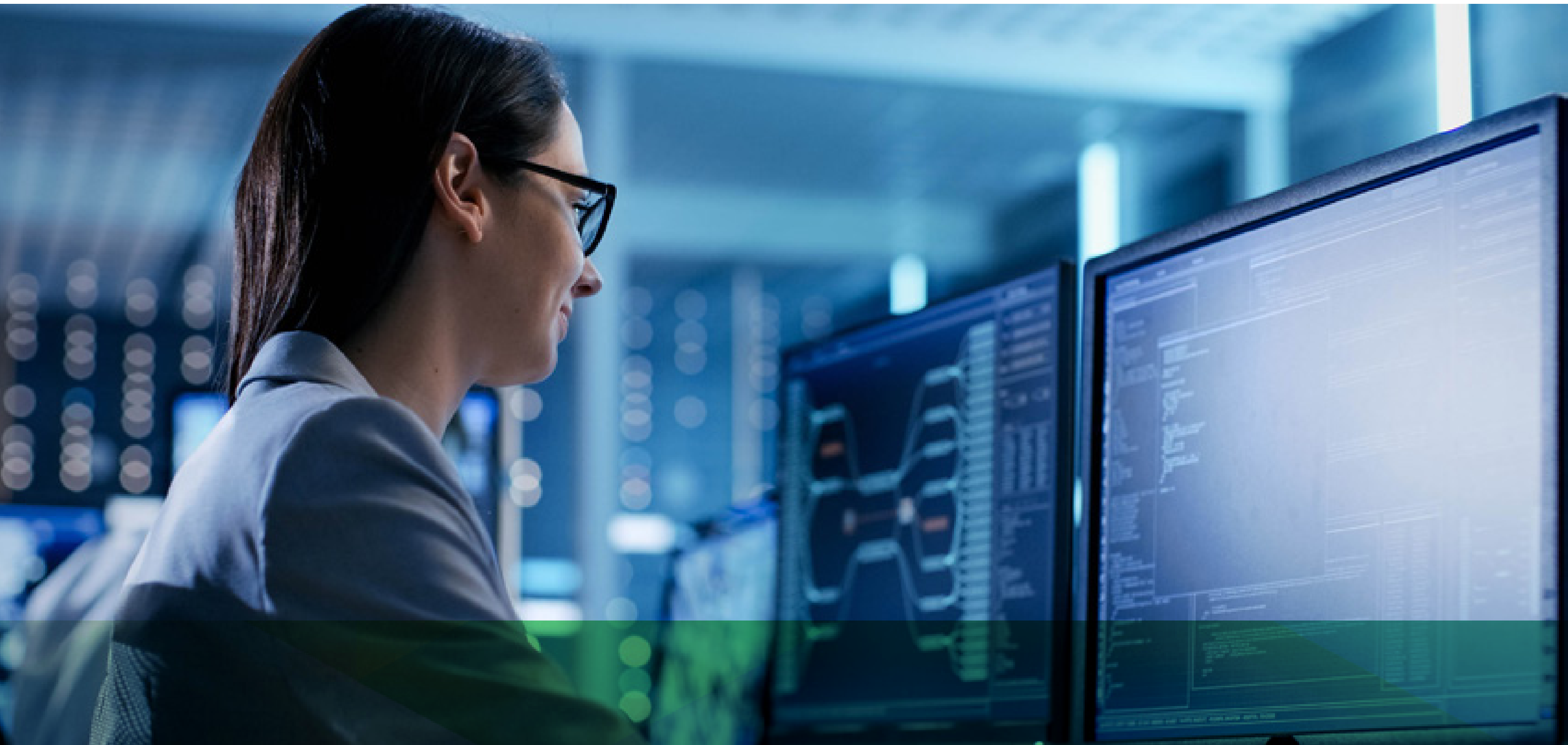
Cybersecurity professionals are cautious about where they choose to work, and active jobseekers are less likely to work for an employer that doesn't take security seriously. Still, 54% of respondents looking for new employment said they would take a job where a breach has already occurred. That number increases to 64% if the breach has been publicly disclosed. Clearly, jobseekers believe they can contribute to improving an organization's security posture. It's information employers can leverage in wooing candidates.

More tenured and manager-level employees are more likely to work where breaches have occurred. The same goes for those actively looking for new employment. This may reflect a higher level of acceptance among more experienced workers who have likely seen breaches occur. Of those with no plans to look for a new job, less than one third (29%) would not work for a company that has been breached.

Figure 3 – Taking a Job Where a Breach Occurred

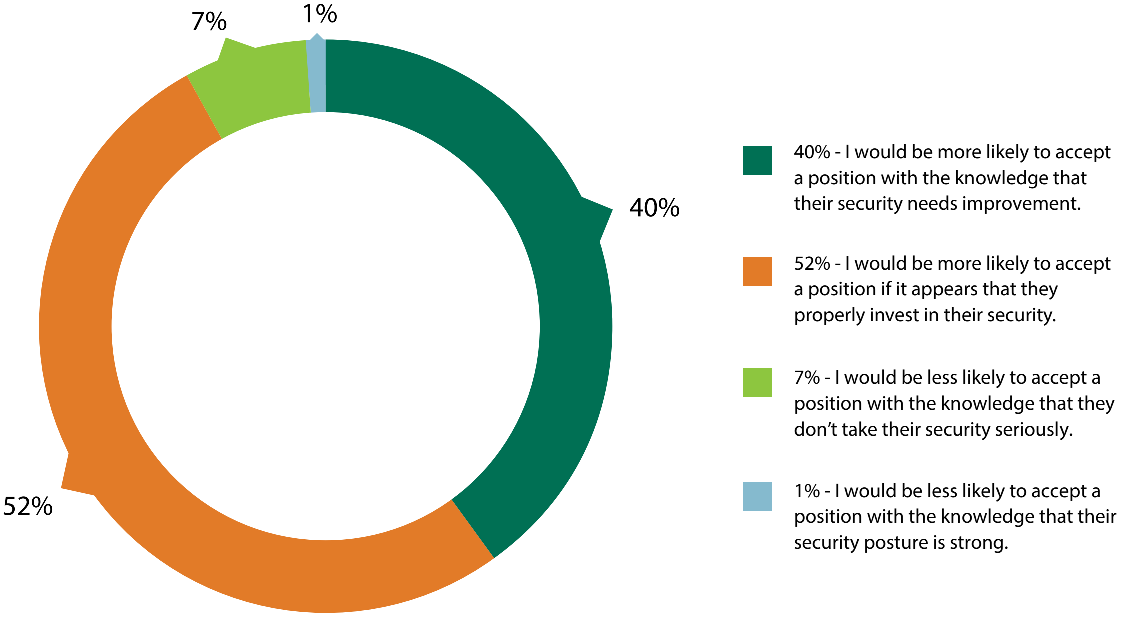


Data suggests cybersecurity professionals are willing to take a position with a company that has been breached. Notably, 19% of directors and middle-managers said 'yes' to working for breached company, but 73% of them said only if the breach was public disclosed in a timely manner. This underscores how experienced cybersecurity professionals advancing in their careers may view the social responsibility and ethical obligations of potential employers.



Despite the willingness to work where security incidents have occurred, jobseekers don't want to step in blindly. For instance, 85% say they would investigate a potential employer's security capabilities before taking a job, and the results would affect their decision. 52% said they are more likely to take a job with a company that properly invests in cybersecurity, and 40% said they would work for a company that needs improvement.

Figure 4 – Investigating Employers' Security Capabilities



While more than half of cybersecurity professionals said they would be more likely to take a position knowing that an organization properly invests in security, 40% were willing to take on a challenge and accept a role with an employer that needs to improve its security.

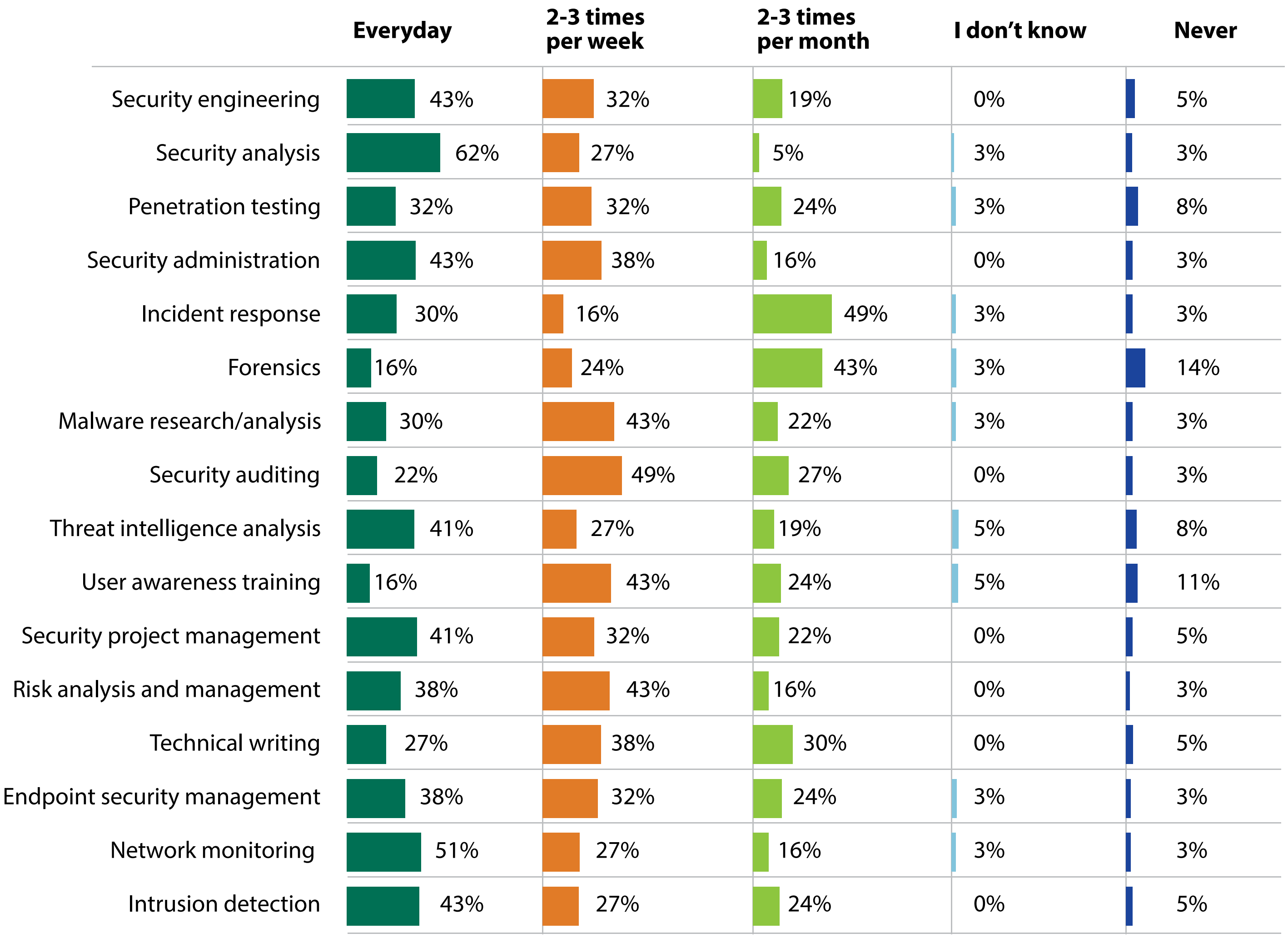
DEEP DIVE: THE SKILLS THEY BRING

When advertising a cybersecurity position, the job description is critical. Candidates draw inferences about the employer's cybersecurity awareness from the job description. More than half (52%) say lack of clarity in a description implies the organization doesn't understand security. Vague language and descriptions that don't seem to accurately reflect the job are definite turnoffs.

Employers and recruiters, therefore, must have a sense of what the job entails, the skills required and the skills cybersecurity professionals are likely to bring. Here are the top five skills the (ISC)^2 study reveals are most commonly used among survey respondents:

1. Cybersecurity Strategy
2. Cybersecurity Management
3. User Education
4. Risk Assessment
5. Security Operations

Figure 5 – Most Commonly Used Cybersecurity Skills



Understanding what activities and what skillsets cybersecurity professionals use most can aid employers when creating job descriptions and defining areas of responsibilities for workers. Security analysis ranked top for an everyday skill, but professionals seem to be struggling to find the time for user awareness training, which they say is an important quality they look for in employers.

WHAT KEEPS THEM BUSY?

Knowing what takes up cybersecurity professionals' time can help employers and recruiters prepare effective job descriptions. For instance, it's helpful to know that active jobseekers spend more time on user awareness training than any other group of surveyed workers.

Here are the skills used most on a daily basis:

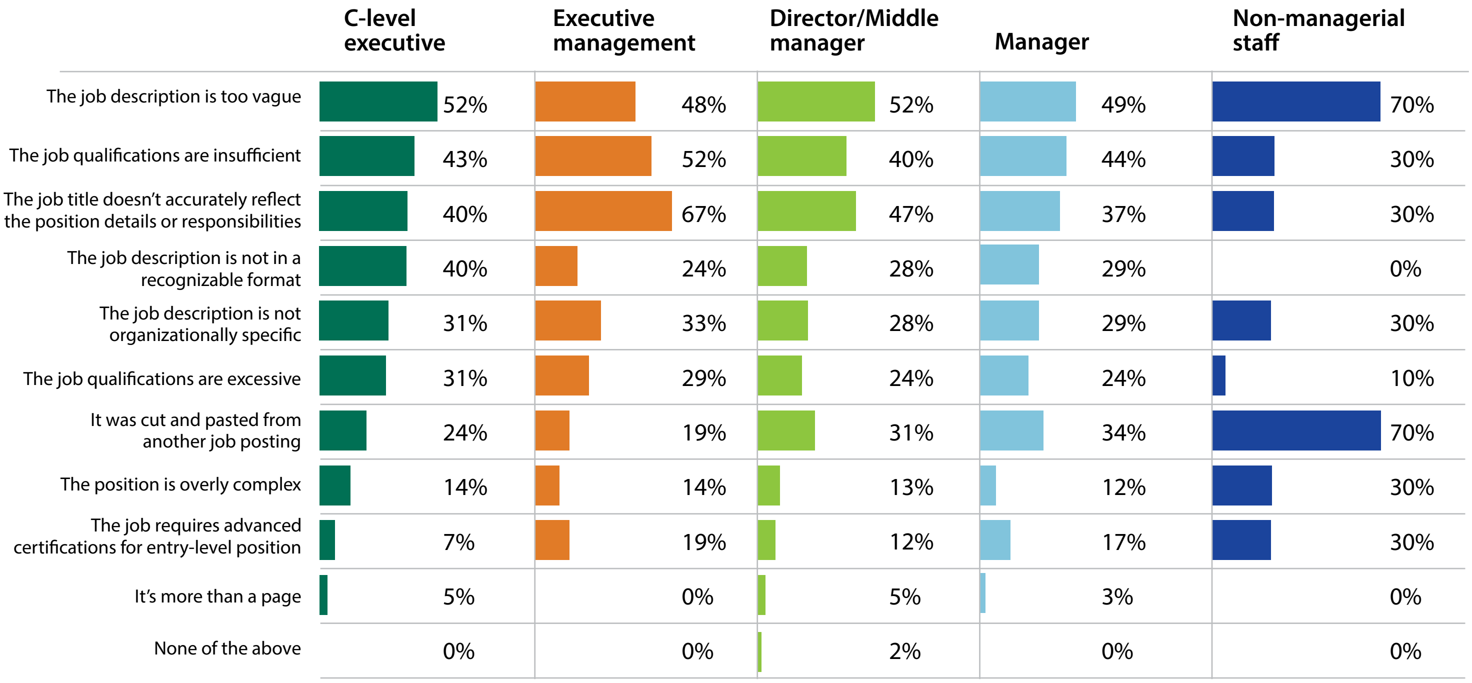
1. Network Monitoring	58%
2. Security Analysis	53%
3. Security Administration	53%
4. Intrusion Detection	47%
5. Risk Analysis and Management	39%
6. Security Analysis	39%

WHAT JOBSEEKERS WANT

Whenever demand is high for talent, the natural inclination is to lure candidates with high salaries. But while salary does matter to cybersecurity jobseekers, it typically isn't the deciding factor. Cybersecurity professionals get their cues about whether an employer suits them from things like the job description and whether the role for which they're being recruited is clearly defined.

Writing job descriptions to match required skills increases an employer's chances of finding the right candidate. Not all candidates can deliver every skill, so avoid using a "kitchen sink" approach in job descriptions. It's a turn-off to seasoned jobseekers. The key takeaway for employers is to recognize that they must be realistic about what a single candidate can bring to the table and be smart about building a well-rounded cybersecurity team across skillsets and disciplines.

Figure 6 – When Job Descriptions Fail



Cybersecurity professionals at all levels are easily turned off by poorly written job descriptions. When asked what about a job description demonstrates an employer's lack of cybersecurity knowledge, respondents cited job descriptions that were vague, included insufficient or excessive qualifications, and those that require advanced certifications for entry-level positions.

More than anything, employers need to demonstrate willingness to listen. Keep in mind the role of cybersecurity workers is in many ways advisory and consultative; they want to be heard. A company's cybersecurity stance depends on it.

The study found 68% of respondents want to work where their opinions are taken seriously and that currently, 54% are satisfied with that aspect of their jobs. That's a gap of 14 percentage points. 62% want to work "where I can protect people and their data," and 58% expressed satisfaction in this regard, a four-point gap. 59% want an employer "that adheres to a code of ethics," and 54% are satisfied, a five-point gap.

Interestingly, there was a 10-point gap when participants were asked about "best salary," but salary ranked lower than these other attributes, with 49% saying they want the best salary vs. 39% who are satisfied. Still, you can't entirely dismiss salary as a factor, taking into consideration 55% of cybersecurity workers with no plans to look for a job are satisfied with their salaries.

Understanding these gaps creates unique perspectives for employers and offers insight into developing more targeted and effective outreach. For example, a TURF analysis of survey data reveals a list of the most optimal groupings of attributes, terms of reach and frequency based on qualified responses.

To project a favorable impression of your organization to cybersecurity jobseekers, stress a combination of these attributes:

1. Your organization invests in the latest emerging security technologies
2. Your organization views cybersecurity more broadly than just technology
3. Your organization invests in training and certification for cybersecurity employees

To align your ideal hire with what cybersecurity jobseekers view as best describing the value they bring to your organization, stress the following responsibilities for the position:

1. Develop cybersecurity strategy
2. Analyze business processes for risk assessment
3. Educate users about cybersecurity best practices

POWER OF THREE

Data suggestions you can make your organization and job descriptions attractive to the most cybersecurity professionals by focusing on a narrow set of attributes.

To project a favorable impression to jobseekers, stress the following:

1 You invest in the latest emerging security tech

2 You view cybersecurity more broadly than just tech

3 You invest in security training and certification

PERFORMANCE REVIEWS

Cybersecurity workers have very definite ideas about how employers should evaluate their performance. They don't believe whether they've stopped a breach is the best way to judge their effectiveness. There was an 11-point gap between how many respondents (16%) believe that should be the case and how they perceive their organizations (25%) prioritize it.

Instead, cybersecurity professionals believe they should be judged on other criteria, including:

- How quickly they respond to incidents
- How efficiently they handle remediation
- Employee awareness levels

Employers should develop a clear measuring stick for cybersecurity success within their organizations. Ambiguity may only lead to low satisfaction and confusion with existing staff, and an insurmountable challenge when recruiting talent unclear on how they can succeed within the organization.

MISSION-ORIENTED

Cybersecurity workers have a strong sense of duty and understand the weight of their responsibilities, which helps explain why they are attracted to companies with strong ethics and a moral compass set to protect people and their data. Employers should know cybersecurity professionals highly value the following attributes in an organization:

- Views cybersecurity more broadly than just technology
- Invests in the latest emerging security technologies
- Invests in training and certification for cybersecurity employees

62%
want to work where
"I can protect people and their data"

These attributes help put into context cybersecurity professionals' disinclination to be judged on whether they can stop a breach. If a company doesn't make the necessary investments in technology or the people in charge of managing security, that affects the security team's ability to prevent a breach.

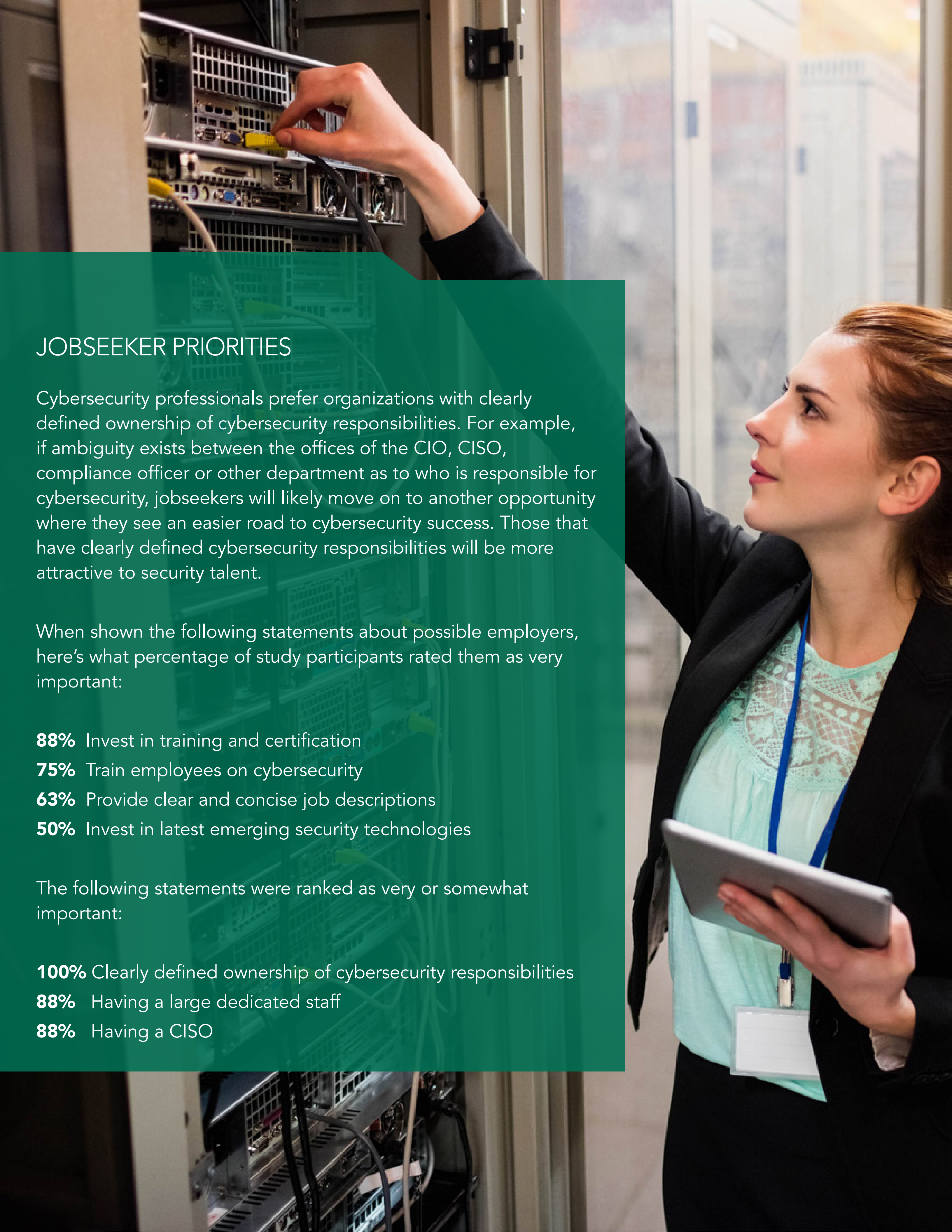
It's no wonder cybersecurity pros want their opinions to be taken seriously (68%) at a company that allows them to protect data and people (62%). If management ignores their recommendations, and then blames them when a breach occurs, they are justified in feeling judged for the wrong reasons.

TENURE EFFECT

How long a cybersecurity pro spends at a company shapes their views of what's important in an employer. For instance, adhering to a strong code of ethics is important to 59% of respondents, but if you look at data trends from entry-level participants, it's 100%. Ethics loses some importance after the first year, but picks up again after the sixth year, leveling off in the mid 60% range.

The study revealed similar attitudes in regard to an organization having "a strong mission that benefits society," which 50% cited as important. As with ethics, these numbers are higher at the entry level, but then taper off.

In contrast, company attributes that rank lower in priority include "best salary" (49%), "flexible working arrangements" (46%), "near work and family" (38%), and "produce a cool product" (35%). A "cool product" takes on more importance after six years, when presumably workers can be choosier about their employment after having acquired some experience. Being near work and family also takes on more importance the longer they stay with a company and establish roots.



JOBSEEKER PRIORITIES

Cybersecurity professionals prefer organizations with clearly defined ownership of cybersecurity responsibilities. For example, if ambiguity exists between the offices of the CIO, CISO, compliance officer or other department as to who is responsible for cybersecurity, jobseekers will likely move on to another opportunity where they see an easier road to cybersecurity success. Those that have clearly defined cybersecurity responsibilities will be more attractive to security talent.

When shown the following statements about possible employers, here's what percentage of study participants rated them as very important:

88% Invest in training and certification
75% Train employees on cybersecurity
63% Provide clear and concise job descriptions
50% Invest in latest emerging security technologies

The following statements were ranked as very or somewhat important:

100% Clearly defined ownership of cybersecurity responsibilities
88% Having a large dedicated staff
88% Having a CISO

WHO ARE THEY?

100% of the participants in the (ISC)^2 jobseeker study consider cybersecurity their primary job function. The study polled cybersecurity at various seniority levels: 17% were C-level executives, 47% middle managers and 28% managers or non-managerial staff.

Here's a breakdown of how long participants have been in their current jobs:

Less than 1 year	1%
1-3	8%
3-6	25%
6-10	30%
10-20	31%
20 or more	4%

Participants work in various industries, but the biggest group was IT (30%), followed by computer software (14%), banking/financial (7%) and retail/wholesale (7%).

68% of respondents were male, and 32% were female, with an average age of 38 and 37, respectively. 76% are in the United States and 24% in Canada.

CONCLUSION

It's clear from the (ISC)^2 study of cybersecurity jobseeker trends that employers face an uphill climb with recruitment. Jobseekers can afford to be choosy because demand is high. They want assurances their employer will treat them properly, listening to their advice and making serious investments in cybersecurity. The more employers understand cybersecurity professionals' priorities, the more likely they are to attract and retain top cybersecurity talent.

METHODOLOGY

Findings are based on a blind survey of 250 cybersecurity professionals within the United States and Canada conducted by Market Cube, LLC, on behalf of (ISC)^2 in December 2017.

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 130,000 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.

This report contains information of facts relating to parties other than (ISC)². Although the information has been obtained from, and is based on sources that (ISC)² believes to be reliable, (ISC)² does not guarantee the accuracy, and any such information might be incomplete or condensed. Any estimates included in this report constitute (ISC)²'s judgment as of the date of compilation, and are subject to change without notice. This report is for information purposes only. All responsibility for any interpretations or actions based on the information or commentary contained within this report lie solely with the recipient. (ISC)² makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy, completeness, and improper or incorrect usage of any information contained in this document.

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.