Building a Resilient Cybersecurity Culture

A dedicated staff with a clear mission helps retain and engage a cybersecurity workforce

(ISC)²®

Inspiring a Safe and Secure Cyber World

INTRODUCTION

By now, nearly everyone in the industry is aware of the cybersecurity workforce gap and has discussed its causes extensively. (ISC)² sought to learn about solutions to the problem from a demographic that may be on the winning side of the equation – companies that report they have all the cybersecurity experts that they need to be successful.

Organizations that make a strong investment in cybersecurity technology, acquire the requisite expertise and follow best practices have a higher level of confidence in their defenses against cybersecurity threats. These organizations enjoy a strong cybersecurity commitment from top management, which enables them to better protect themselves and prevent their cybersecurity workers from seeking employment elsewhere, according to the new Building a Resilient Cybersecurity Culture study by (ISC)².

The study focused on 250 companies of various sizes with a solid cybersecurity track record; 100% of respondents say their organization does an adequate job of ensuring it has "enough cybersecurity expertise on staff." The study set out to determine what they do to better prepare their defenses against cybersecurity threats so other organizations can learn from them how to better secure their critical assets.

STRONG CULTURE BEGETS FOCUS

Of special interest was how these companies overcome the ongoing challenge of finding and retaining cybersecurity talent in a market where demand outstrips supply. Only 18% of study participants worry about losing their security employees to other companies, an especially significant finding considering 84% of cybersecurity professionals polled in December 2017 by (ISC)[2] said they were open to new opportunities.

In fact, respondents in the survey worry less about losing cybersecurity employees than actual threats, an indication that having competent, experienced people in place allows them to focus on what is important – protecting the organization. Hence, 57% say their biggest concern is the constant evolution of threats they face, and 43% say it's the determination of threat actors.

WHO ARE THEY?

All 250 participants in the study are full-time employees of their companies, have cybersecurity responsibilities, and believe their organizations do an adequate job of properly staffing their cybersecurity teams.

99% indicate that they have influence or decision-making authority in hiring and evaluating IT professionals.

84% of respondents hail from organizations with more than 100 employees.

16% work at companies with 100 or fewer.

Other major findings of the study:

- A strong cybersecurity culture translates to a higher focus on hiring certified professionals and conducting internal cybersecurity training
- 97% say top management understands the importance of strong cybersecurity
- 96% indicate their policies align with their board of directors' cybersecurity strategy
- 86% of companies properly staffed with cybersecurity expertise employ a Chief Information Security Officer (CISO)

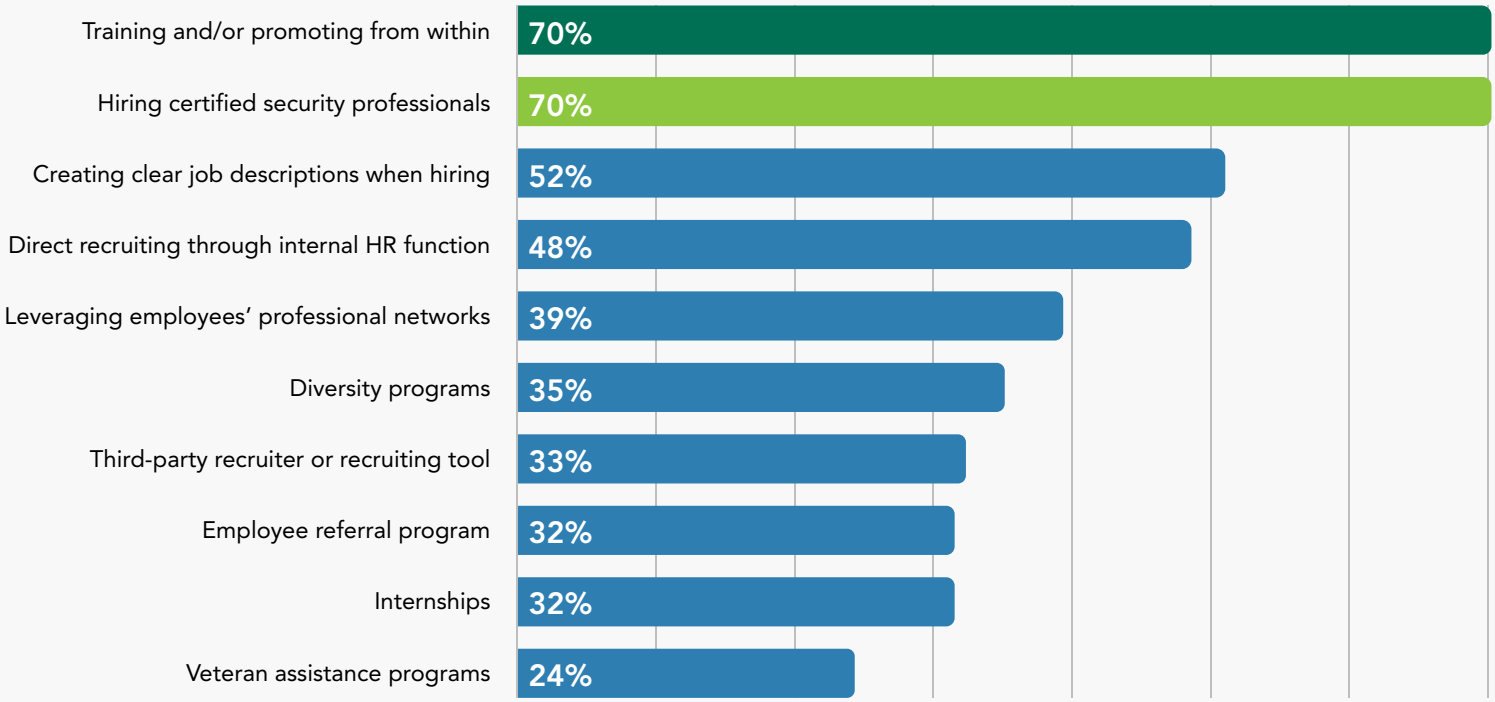
INVESTING IN TECHNOLOGY AND PEOPLE

In building their cybersecurity teams, organizations in the study give priority to the following:

- Hiring certified security professionals (70%)
- Training and promoting from within (70%)
- Drafting clear job descriptions when hiring (52%)

The third point is especially eye-catching because jobseekers have identified it as an issue. In (ISC)²'s January 2018 report Hiring and Retaining Top Cybersecurity Talent, lack of clarity in job descriptions was a top complaint among cybersecurity jobseekers, with 52% saying unclear job ads show a lack of understanding of security.

Hire Smart, Train Hard



Respondents were asked which tactics are most effective in building an internal cybersecurity team. The results indicate that the keys are hiring smart and being prepared to provide continued training and promotional opportunities to security staff.

To strengthen their security teams once built, participants in the survey place a strong emphasis on offering training and certification opportunities to employees (57%), followed by cross-training on cybersecurity skills and responsibilities (55%). Attracting the right talent ranks lower (48%), which implies these organizations are confident in their ability to retain and properly train their cybersecurity professionals.

Interestingly, investing in technology ranks highest on the list (62%), so even though they view skills development as important, these companies do not overlook the need to invest in the right technology tools.

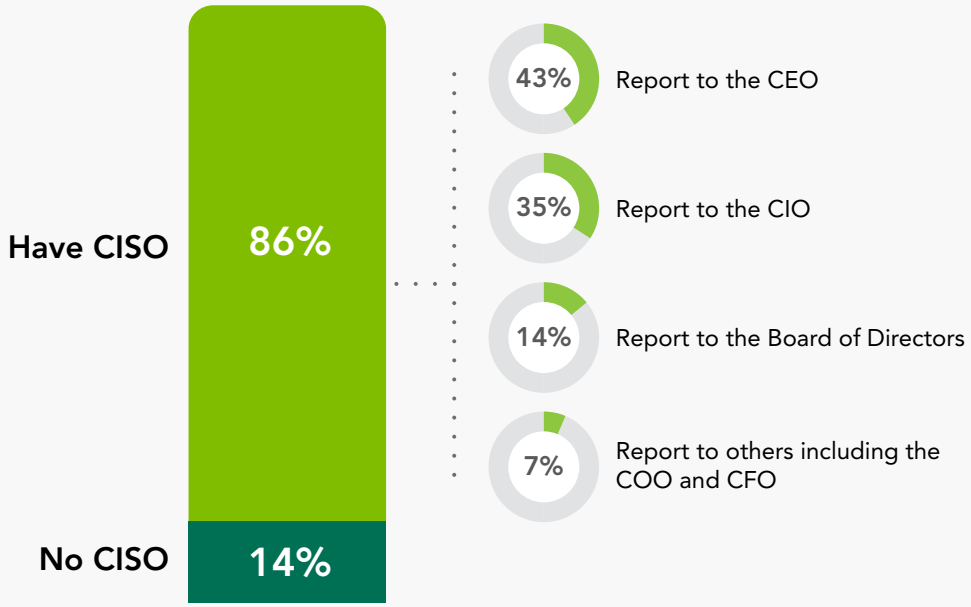
CYBERSECURITY AS A PRIORITY

Slightly more than half of survey participants (51%) indicate their company employs a dedicated cybersecurity staff, which they believe is critical to cyber readiness. The study also revealed that 86% of organizations that consider themselves adequately staffed with cybersecurity talent employ a CISO. This compares to 49% of companies overall that have a CISO, according to other research.

The CISO position has spurred controversy over the years, with top management in many companies viewing it as a scapegoat for security breaches. CISOs often feel undervalued or ignored, which helps explain why their average tenure is two to four years. But (ISC)²'s study indicates that organizations that properly utilize and empower a CISO find they can contribute to a strong cybersecurity culture.

Interestingly, reporting structures for CISOs varied. 14% report directly to the Board of Directors. 35% and 43%, reported to the CIO and CEO, respectively. This indicates that who the CISO reports to may be less important than ensuring they have the ability and resources to influence change and make cybersecurity a strategic priority.

CISO Reporting Structure



Successful organizations overwhelmingly report that they employ a CISO, and in many cases, that person reports directly to either the CEO or the Board of Directors.

FITTING RIGHT IN

Respondents said the top five attributes they view as important for a team member to have are:

- Skill and knowledge with our technology **(72%)**
- Knowledge of security best practices **(65%)**
- Understanding of our processes, data flows and controls **(63%)**
- Understanding of cutting-edge technology solutions **(60%)**
- Ability to educate users on security best practices **(53%)**

This aligns with two other significant findings. The overwhelming majority of respondents (96%) say their organizations' policies are in line with the security strategy set by their board of directors. And not surprisingly, 97% say their entire executive management team "understands the importance of strong security practices and reinforces those messages with staff."

Corporate commitment to cybersecurity appears to have an effect on the tenure of cybersecurity employees. A solid majority of companies in the survey (79%) enjoy an average tenure of three years or more. In 37% of organizations, the average surpasses five years. Considering that cybersecurity pros are contacted by recruiters on a regular basis, this is a significant achievement.

GOVERNMENT AS A TALENT SOURCE

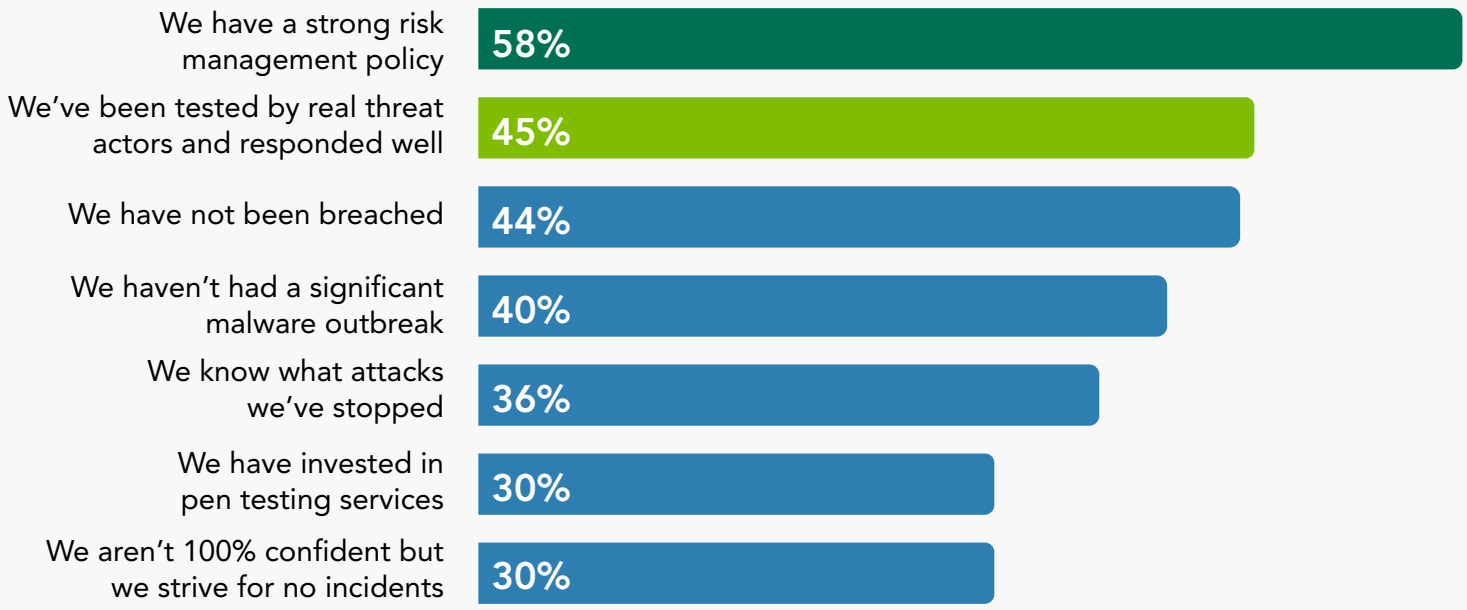
As (ISC)[2] found in the January 2018 jobseeker study, cybersecurity professionals are less motivated by salary than employer attributes such as taking the work of cybersecurity staff seriously and adhering to a code of ethics. But the study identified an exception – cybersecurity recruits from government agencies.

The new study finds that 50% of organizations have successfully recruited talent from the government ranks; they know these workers typically undergo extensive training to fight against nation-state threat actors and organized cybercrime. One of the biggest draws to private industry, according to 67% of respondents, is salary. It's no secret private companies generally pay better than government agencies, so it stands to reason many recruits from the government would welcome higher pay. Other deciding factors for government recruits include having a great leadership team (60%) and working for a mission-based organization (59%).

WHY SO CONFIDENT?

Having the right people in place to manage cybersecurity, backed by a strong commitment from the top, has a positive effect on an organization's confidence to defend against threats. This is evident in answers to the question, "What indications do you have that your capabilities are adequate to protect the enterprise?" The top answer (58%) is a strong risk management policy.

Where Confidence Stems From



When asked why they believe their team's capabilities are adequate to protect the enterprise, respondents pointed to the development of strong risk management policies and the knowledge that they have already successfully thwarted attacks.

SETTING AN EXAMPLE

The Building a Resilient Cybersecurity Culture study confirms that organizations following best practices in hiring and retaining top talent, gaining top management's awareness and recognition for the importance of cybersecurity, and aligning policies with corporate strategy can create more confident, effective and resilient cybersecurity teams. Companies still struggling with unfocused cybersecurity strategy, uncertainty in their cybersecurity readiness or that are unable to retain their security staff should consider modeling themselves after these organizations.

METHODOLOGY

Findings are based on a blind survey of 250 cybersecurity professionals within the United States conducted by Market Cube, LLC, on behalf of (ISC)² in August 2018.

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. 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.

Inspiring a Safe and Secure Cyber World