FORTINET

REPORT

Fortinet Survey Finds Widespread Impact from Cybersecurity Skills Shortage

Table of Contents

Executive Summary 3

Infographic: Key Findings. 4

Introduction 5

Methodology for This Study. 5

Cybersecurity Skills Gap Trends 6

The Cybersecurity Skills Shortage Impacts Organizations of All Types 6

Technology-focused Certifications Can Help Bridge the Gap 8

Veterans Are Already Filling Gaps, and Can Fill Even More 10

Conclusion 13

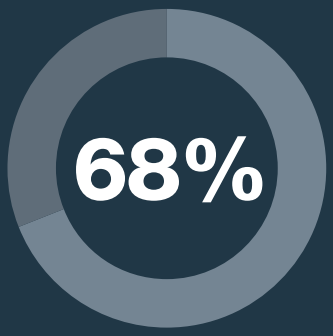
Executive Summary

This report is based on a survey of security leaders across North America, covering the cybersecurity skills shortage and potential ways to address it. The findings indicate that the skills gap is still very real, impacts a wide variety of companies, and has been at least partly responsible for one or more intrusions or breaches in the past year at a majority of organizations. Organizations can do more to recruit nontraditional candidates to the cybersecurity field, if they are to address the shortage of skilled professionals.

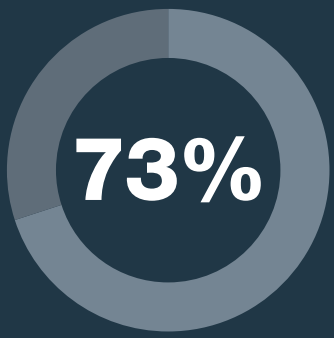
Recruitment of nontraditional candidates into cybersecurity requires a holistic look at the workforce. Bridging the skills gap requires the development of new candidates through education, upskilling current IT professionals, and developing new skills of the existing workforce. This survey explores the upskilling of IT professionals and re-skilling of former military service members as a way to close the cybersecurity skills gap.

Certifications have shown to increase knowledge and skills of individuals already in or entering the cybersecurity field. Employers have seen how certifications prepare workers from IT roles to take on cybersecurity responsibilities within their organizations. Certifications also enable individuals to diversify their skill set and oftentimes propel themselves to greater career growth. Military veterans and military spouses are another group within the workforce that can be instrumental in reducing the cybersecurity talent shortage. Organizations that have a dedicated focus on military recruitment have benefited from teams with diverse perspectives and skill sets that complement a career in cybersecurity.

Infographic: Key Findings



of organizations struggle to recruit, hire, and retain cybersecurity talent



of organizations had at least one intrusion/breach over the past year that can be partially attributed to a gap in cybersecurity skills. **47%** had three or more.

Most-cited hard-to-hire position: **Cloud Security Architect**

85%
of respondents have team members with security certifications

94%
believe that their certifications have better prepared them for their current role

82%
of organizations prefer to hire candidates with certifications

57% of U.S. cybersecurity teams hired at least one veteran

43% of U.S. organizations have a C-suite executive who is a veteran or a military spouse

49% have a focused hiring program targeting veterans

40% measure how much business they do with third-party, veteran-owned businesses

Introduction

The cybersecurity skills shortage continues to be a reality, and research indicates the skills shortage continues to worsen. The (ISC)[2] Cybersecurity Workforce Study, released in 2019, concluded 4.07 million workers would now need to be added to the 2.8 million currently in the field globally to fully close the gap.[1]

With the workforce being more distributed than ever before as a result of the COVID-19 pandemic, millions of workers around the world will continue to depend on remote access for months—or even years—after economies begin reopening.[2] As infrastructures continue to become even more distributed, governments, academia, and businesses will continue to need IT professionals with broad cybersecurity skills to properly secure their organizations.

The Role of Digital Innovation

Digital innovation initiatives have exacerbated the skills shortage, expanding organizations' IT ecosystems—and therefore their attack surface—and the need for specialized talent to protect these investments. In other words, while the number of cybersecurity professionals is increasing, demand is increasing even more quickly.

Small and midsize businesses and smaller enterprises bear the brunt of the skills gap, as large organizations with brand equity can often outbid them to acquire talent.[3] At the same time, smaller organizations are increasingly attractive targets for cyber criminals—often as a backdoor way of infiltrating their large enterprise customers and partners.[4] Regardless of the impact to each organization, it is clear that no single solution will be adequate to close the skills gap. Organizations will need to be creative in crafting a multifaceted approach to staffing an increasingly critical function.

Methodology for This Study

This report is based on a survey commissioned by Fortinet and conducted in early March, 2020. Respondents were located in the United States and Canada, work at companies with 2,500 or more employees, and are responsible for cybersecurity at their organizations. Job grades ranged from director to C-level, including titles such as CIO, CISO, COO, and vice presidents or directors of IT, the security operations center (SOC), and the network operations center (NOC) vice president or director.

The questions in the survey explore the extent and impact of the cybersecurity skills shortage on respondents' organizations. They also investigate two areas that organizations might use to find cybersecurity talent by unconventional means—promoting cybersecurity certification programs and recruiting military veterans. We will discuss three trends that result from analysis of this research.

"The talent crisis is real, and as an industry, we can't wait years for a solution."[5]

Cybersecurity Skills Gap Trends

Trend: The Cybersecurity Skills Shortage Impacts Organizations of All Types

Respondents to the Fortinet survey confirm what has been reported elsewhere: The impact of the cybersecurity skills shortage severely impacts a broad cross-section of organizations. More than two-thirds of respondents (68%) report that their companies struggle to recruit, hire, and retain cybersecurity talent (Figure 1). The problem is even more acute in Canada, where 78% of respondents report such a struggle. These struggles create real problems for organizations; more than three-quarters (76%) of respondents say that a shortage of skilled security professionals creates additional risks for their organizations.

These risks are not just theoretical. Nearly three-quarters (73%) of organizations represented in the survey had at least one intrusion or breach over the past year that can be partially attributed to a gap in cybersecurity skills (Figure 2). And nearly half (47%) had as many as three such intrusions in the past 12 months. These results show that the skills shortage is causing real impact for a large number of organizations, creating the potential for the theft of consumers' personal information, private corporate information, and even trade secrets.

When asked about specific roles that are hardest to fill, the most commonly cited job role is cloud security architect, which is cited as among the three hardest roles to fill by half of respondents (Figure 3). This is not surprising, as one recent survey found that 85% of companies now operate in multiple clouds,[6] and integrating security across this sprawling infrastructure is a critical priority. A related role, security architect, was also among the top three hard-to-fill positions cited, likely also because of the increasing complexity of enterprise networks.

The other positions most commonly cited as difficult to fill are more commoditized roles at the entry level—security administrator, SOC specialist, and compliance specialist. These positions are widely advertised on job sites, and organizations do well to be deliberate about employee retention by offering the highest salaries possible, maximizing opportunities for advancement, and providing a healthy work culture.[7]

Figure 1: Recruitment struggles and related cyber risks for organizations.

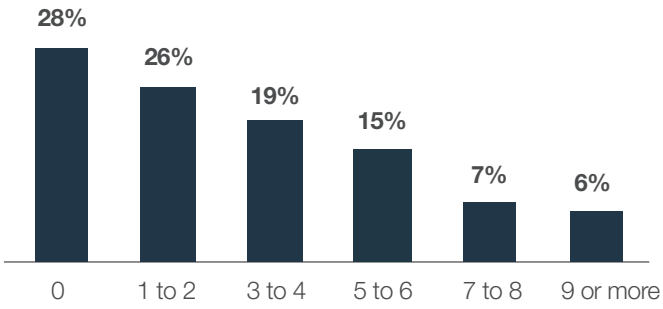


Figure 2: Number of intrusions or breaches attributed to lack of cybersecurity skills on staff.

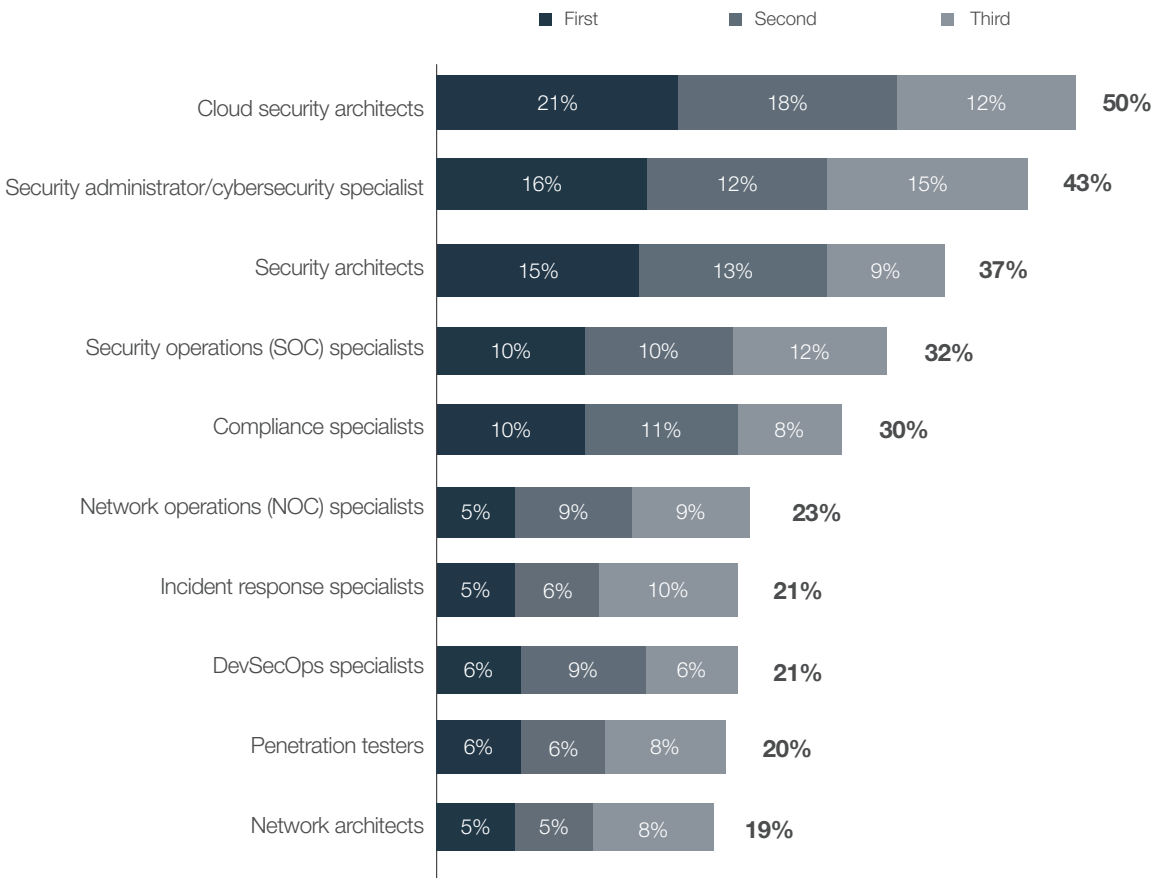


Figure 3: Hardest cybersecurity skill sets/roles to fill.

"Since our lives are now controlled by bits and bytes, the cybersecurity skills shortage is an existential threat to all of us."[8]

Trend: Technology-focused Certification Can Help Bridge the Gap

Today's alarming skills gap means that organizations need to expand their recruitment efforts beyond current cybersecurity workers and traditional talent pools to include individuals with certifications in addition to role-specific degree and certificate programs at colleges and universities. Technology-focused certifications are a tool that can help workers in other professions to develop cybersecurity skills relatively quickly. Among survey respondents, 81% have earned certifications themselves, and 85% report that others on their team have certifications (Figure 4).

There is no ambiguity in the value that security professionals place in the certifications they hold. An astounding 94% of respondents believe that their certifications have better prepared them for their current role (Figure 5). More than half of respondents report that their certifications have increased their cybersecurity awareness and help them perform their duties more effectively. And nearly 4 in 10 (39%) believe that their certifications have accelerated their career growth.

When it comes to hiring and recruitment decisions, 82% of organizations prefer to hire candidates with certifications (Figure 6). When asked for reasons that they prefer certified new hires, more than half find the certifications as validation of the candidate's cybersecurity awareness and knowledge, and this in term increases their confidence that they will perform their duties well.

The data is clear that certifications provide value for IT professionals and those looking to enter the field. Certifications enable professionals to continually update their knowledge and skills to stay current with industry trends and evolving threats. Certifications also allow individuals to learn new knowledge that makes it easier for them to transition into cybersecurity and helps organizations to broaden their recruitment efforts beyond traditional degree requirements.

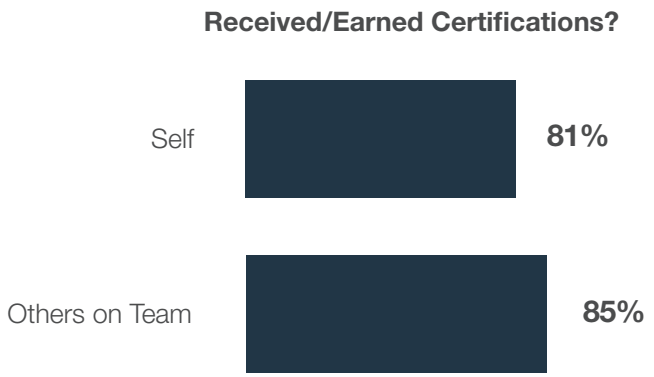


Figure 4: Certifications earned by respondents and team members.

Figure 5: Perceived benefits of certification.

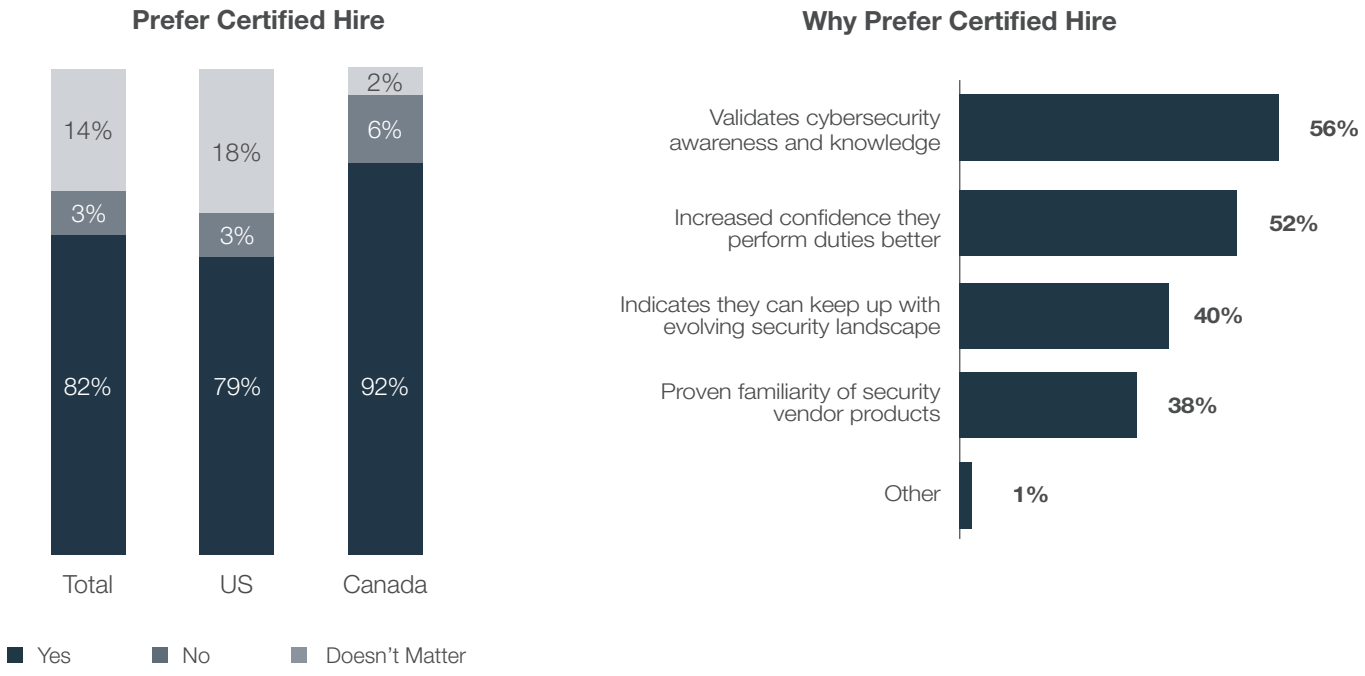


Figure 6: Importance of certifications in hiring.

"Ultimately, a good competitive advantage in the workforce comes from being skilled and accredited in areas where there is a skills shortage."[9]

Trend: Veterans Are Already Filling Gaps, and Can Fill Even More

The United States maintains a large and highly skilled military trained in both conventional and cyber warfare. More than 250,000 service members will leave active duty every year for the next several years, and they will have an average of 15 years of specialized experience under their belts.[10] This pool of talent provides another way to address the cybersecurity skills shortage.

Among U.S. respondents, 57% indicated that their cybersecurity team had hired at least one veteran (Figure 7). Veterans' initial roles at respondents' organizations spanned a number of job titles (Figure 7), but nearly half of them (45%) started their civilian careers as security administrators or SOC specialists (Figure 8).

Interestingly, 43% of U.S. respondents report that at least one C-suite executive at their firm is a veteran or a military spouse (Figure 9). These executives tend to have a long tenure with their company, with 80% having served there for five years or longer. This is an illustration of the caliber of worker that can come from a military background. When asked about stand-out attributes of their veteran colleagues, more than 40% of respondents cited their work ethic, their attention to detail, and their ability to work in fast-paced, high-stress environments (Figure 10). In freeform questions, respondents cited several additional positive attributes in their veteran colleagues, including decision-making abilities, discipline, and a no-quit attitude.

Despite the presence of veterans in cybersecurity workplaces and in executive management, fewer than half (49%) of U.S. respondents report that their organizations have a focused hiring program targeting veterans (Figure 11), while only 22% have a hiring program targeting military spouses (Figure 12). Only 24% have a Military Occupational Specialty Translator to help with veterans' transition from military to civilian life, while 4 in 10 respondents say that their firms have a program in place that measures how much business they do with third-party businesses owned by veterans.

The data is clear that cybersecurity leaders value the veterans and military spouses that work on their teams and across their organizations. However, it is also clear that with a more deliberate effort at the corporate level, organizations could benefit further from the broad and deep skill sets of veterans—making another dent in the cybersecurity skills shortage.

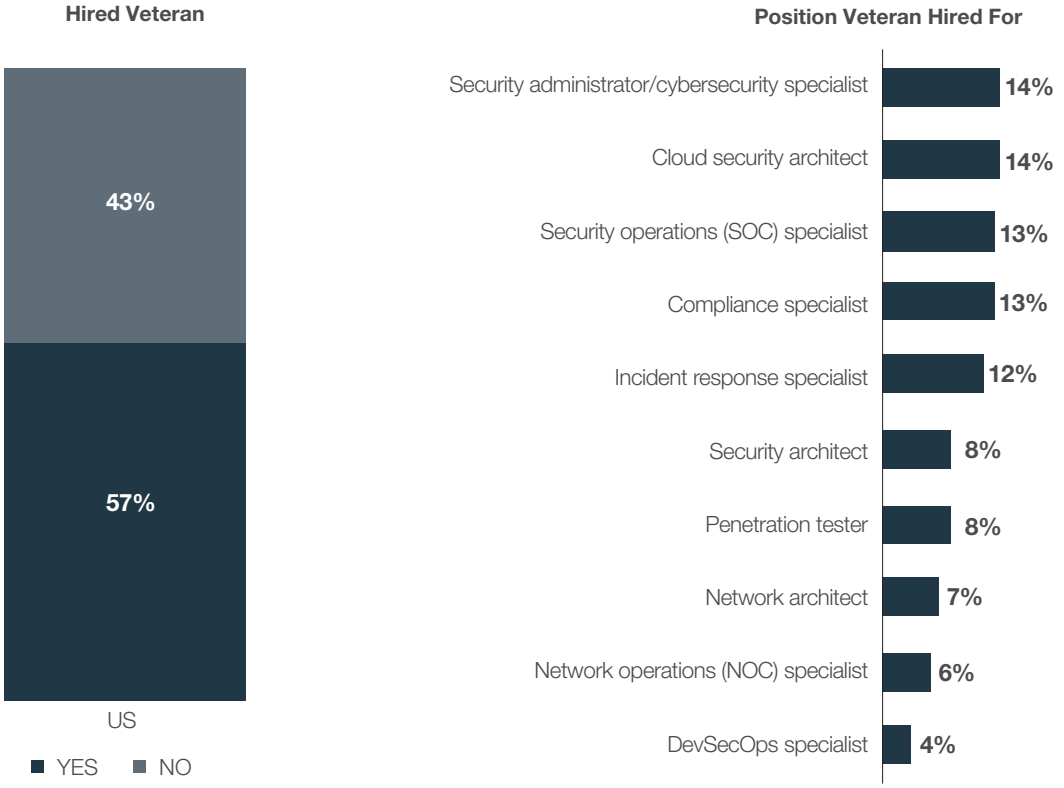


Figure 7: Veterans hired for cybersecurity positions.

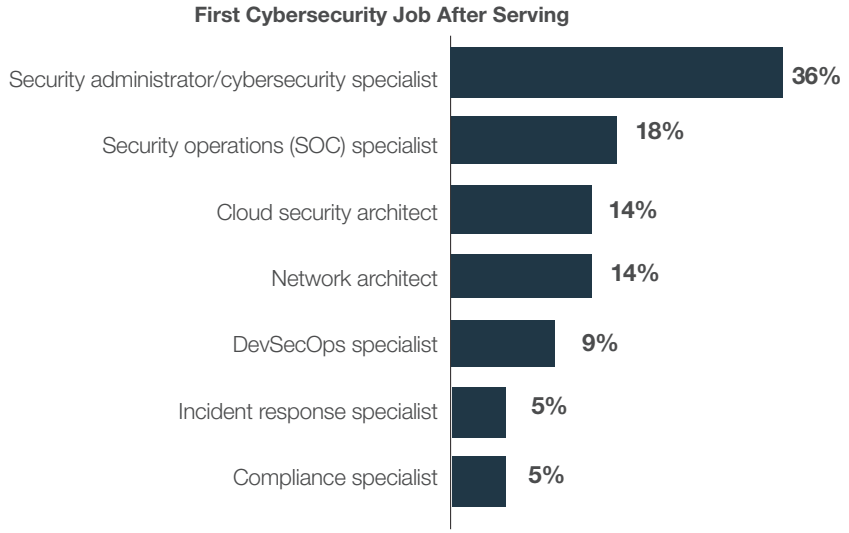


Figure 8: Veteran respondents' first job after serving.

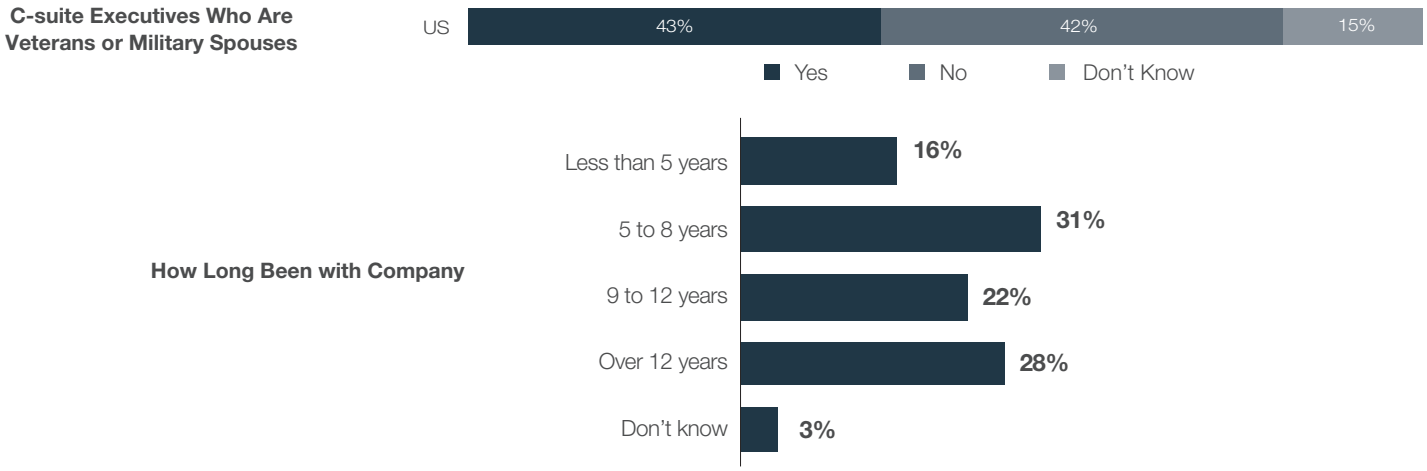


Figure 9: Respondents whose organizations have veterans in the C-suite.

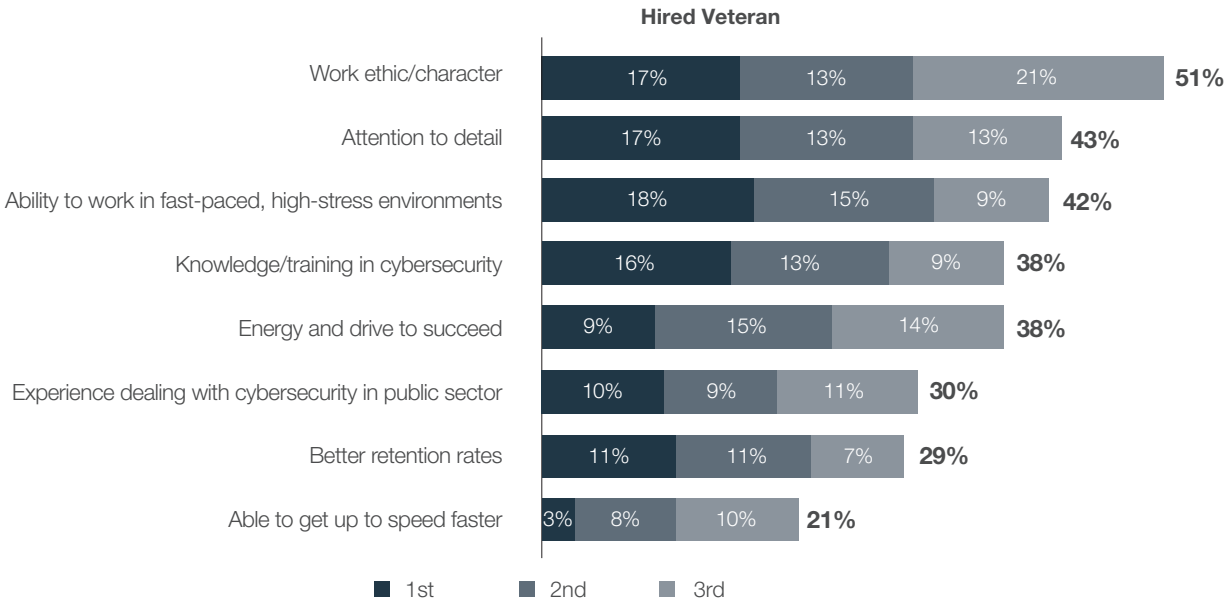


Figure 10: Stand-out attributes of veterans at respondents' organizations.

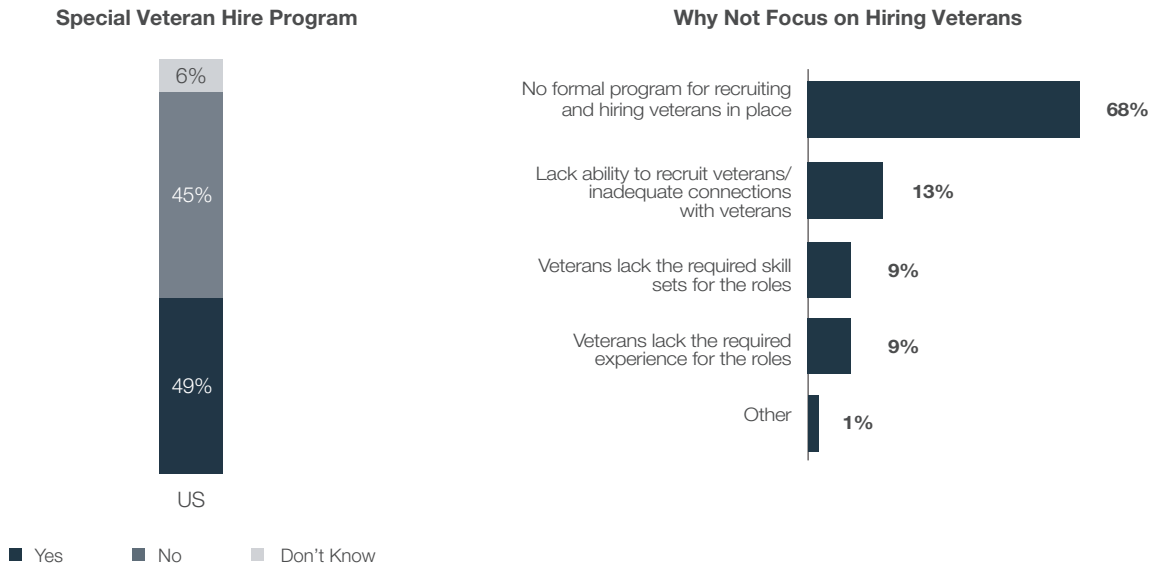


Figure 11: Veteran hiring programs at respondents' companies.

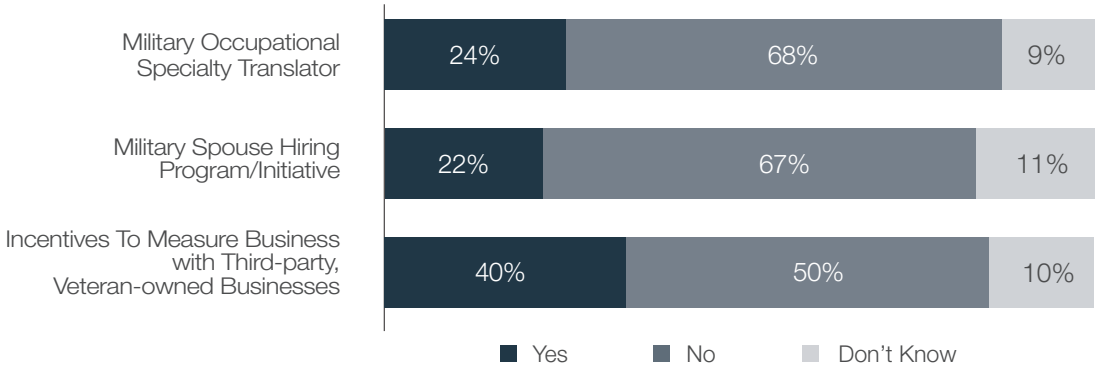


Figure 12: Veteran hiring and contracting incentives in place at respondents' organizations.

"Today's military is highly technical, and many of these men and women have been trained to use some of the most sophisticated technologies running on some of the most highly targeted networks in the world."[11]

Conclusion

Fortinet's survey results clearly indicate that the cybersecurity skills shortage is having a tangible negative impact on a wide variety of organizations. Each firm must respond to the crisis according to its own priorities and risk tolerance, but it is obvious that no single approach is adequate. On the demand side, every dollar spent on technology that makes cybersecurity professionals more productive likely saves many dollars in additional hiring needs. These steps can include the building of a security architecture that is integrated from end to end—from the data center, across multiple clouds, to Internet-of-Things (IoT) devices at the network edge. The use of artificial intelligence to perform less complex security processes also can slow the growth of the required headcount of the cybersecurity team.

On the supply side, efforts to recruit from nontraditional talent pools will also pay dividends in diversifying the skills and perspectives of the team while adding to the total number of cybersecurity workers in the field. Certification programs can give candidates the knowledge they need to perform critical security tasks. Veterans are one group that can potentially provide highly qualified candidates who can hit the ground running in many cases.

Over time, individual companies can also address their own skills shortages by being deliberate about employee retention. Companies that pay above-average salaries and take steps to make their companies healthy and affirming places to work will see less turnover—and less of a cybersecurity skills shortage over time.

Whatever the specific efforts taken by individual organizations, the cybersecurity skills shortage is not going away anytime soon. Companies that deal most effectively with the crisis will take a strategic, multifaceted approach—and this will pay dividends in increased security and higher profitability.

"Organizations are looking at the cybersecurity skills crisis in the wrong way: it is a business, not a technical, issue. Business executives need to acknowledge that they have a key role to play in addressing this problem by investing in their people."[12]

Reference List

[1] "Cybersecurity Workforce Study, 2019: Strategies for Building and Growing Strong Cybersecurity Teams," (ISC)², accessed May 6, 2020.

[2] Dan Raywood, "The Short-Term Impact of COVID-19 on the Cybersecurity Industry," Infosecurity, March 26, 2020.

[3] Brian NeSmith, "The Cybersecurity Talent Gap Is An Industry Crisis," Forbes, August 9, 2018.

[4] "43% of Cyber Attacks Still Target Small Business while Ransomware Stays On the Rise," Small Business Trends, May 22, 2019.

[5] "The State of Cybersecurity Hiring: Recruiting Watchers for the Virtual Walls," Burning Glass, June 2019.

[6] "Assembling your cloud orchestra: A field guide to multicloud management," IBM, accessed May 20, 2020.

[7] Zeljka Zorz, "Traditional cybersecurity staff retention tactics becoming less effective," Help Net Security, March 4, 2019.

[8] Jon Oltsik, "Is the cybersecurity skills shortage getting worse?" CSO, May 10, 2019.

[9] Tony Vizza, quoted in Mirko Zorz, "Exploring the benefits of cybersecurity certification," Help Net Security, October 29, 2019.

[10] Anthony Giandomenico, "Fill Your Cybersecurity Skills Gap With Veterans," CSO, November 12, 2018.

[11] Ibid.

[12] Candy Alexander, quoted in "Cybersecurity Skills Shortage Worsening for Third Year In A Row, Sounding the Alarm for Business Leaders," Information Systems Security Association (ISSA), May 9, 2019.

FORTINET

www.fortinet.com

May 22, 2020 11:02 AM

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:2020:Report-Fortinet-Survey-Skills-Shortage:report-fortinet-survey-skills-shortage

676829-0-0-EN