State of Cybersecurity 2020

Part 1: Global Update on Workforce Efforts and Resources

ISACA

ABSTRACT

State of Cybersecurity 2020 reports the results of the annual ISACA® global *State of Cybersecurity Survey*, conducted in the fourth quarter of 2019. This Part 1 survey report highlights current trends in cybersecurity workforce development, staffing, budgeting and gender diversity. The report echoes—and reaffirms—key findings of prior years: Enterprises are still short-staffed in cybersecurity, struggle to find sufficient talent for open positions and expect their cybersecurity budgets to grow. Efforts to increase the number of women in cybersecurity roles progressed slightly, and more enterprises established gender diversity programs.

CONTENTS

Executive Summary

This year's global *State of Cybersecurity Survey* asked respondents to identify current and anticipated challenges and trends in cybersecurity. This report analyzes survey results specific to cybersecurity workforce development, resources and diversity. In a second (forthcoming) report, ISACA® examines survey results relating to security operations, cyberattacks and threats, and organizational cybersecurity and governance.

The latest *State of Cybersecurity Survey* results are consistent with findings from the previous two years. Enterprises continue to lack the staff required to combat the cyberthreats they face. However, the factors influencing whether candidates are viewed as well qualified shifted, which calls into question traditional pathways to cybersecurity careers. While hiring remains challenging, respondents indicate that retaining cybersecurity talent is even more difficult this year, highlighting the criticality of skills gap mitigations—especially when the workforce shortage continues to rise. Gender diversity efforts are helping to bring more women into the cybersecurity workforce—albeit slowly. Cybersecurity budgets in 2020 are forecast to be higher than 2019 budgets but show signs of leveling off when compared to prior years.

Survey Methodology

In the final quarter of 2019, ISACA sent online survey invitations to a global population of cybersecurity professionals who hold ISACA's Certified Information Security Manager® (CISM®) certification or have information security job titles. Survey data were collected anonymously via SurveyMonkey. A total of 2,051 respondents completed the survey in its entirety, and their responses are included in the results.[1]

The survey presented respondents with multiple-choice and Likert scale-format questions organized into six major sections:

- Hiring and skills
- Diversity
- Security operations
- Cybersecurity budgets
- Cyberattacks and threats
- Organization cybersecurity and governance

The survey's target population consists of individuals who have cybersecurity job responsibilities. Of the 2,051 respondents, 913 indicate that their primary professional area of responsibility is cybersecurity. **Figure 1** captures key demographic norms across a diverse set of survey respondents.

Respondents represent over 17 industries (**figure 2**) and hail from 102 countries.

1 Certain questions included the option to choose "Don't know" from the list of answers. Where appropriate, "Don't know" responses were removed from the calculation of findings. Result percentages are rounded to the nearest integer.

FIGURE 1—RESPONDENT DEMOGRAPHICS

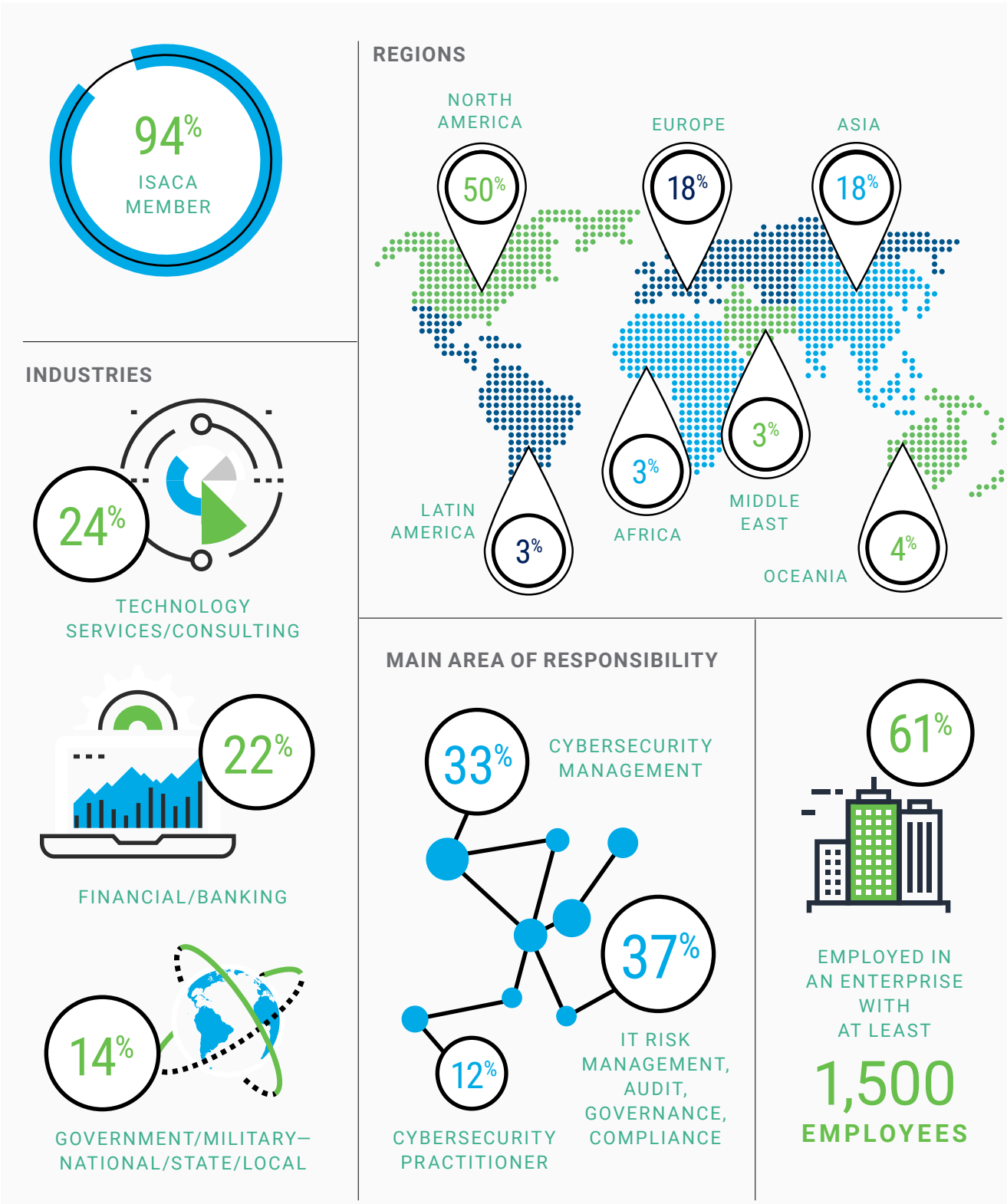
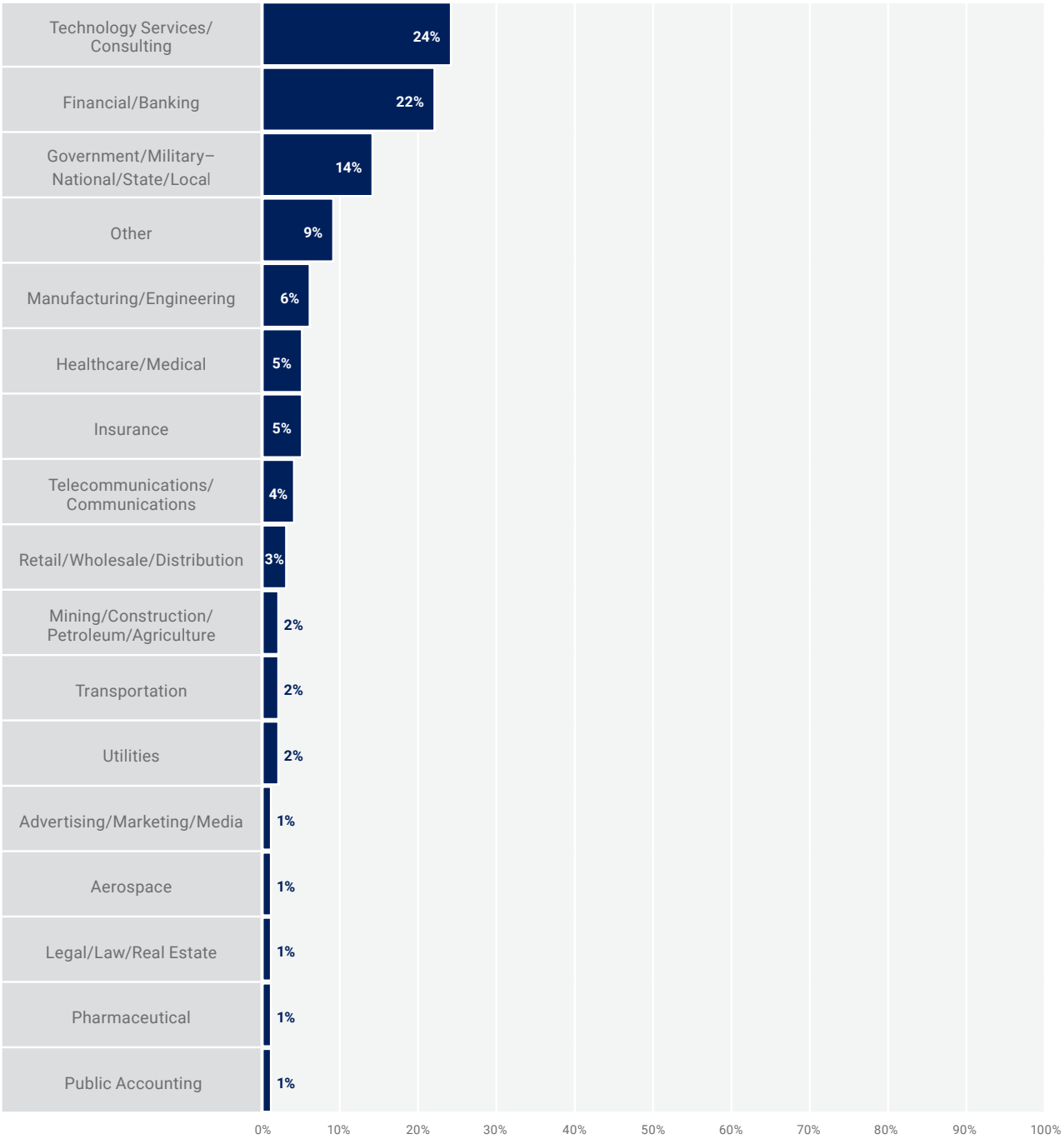


FIGURE 2—INDUSTRY SECTORS

Indicate your organization's primary industry.



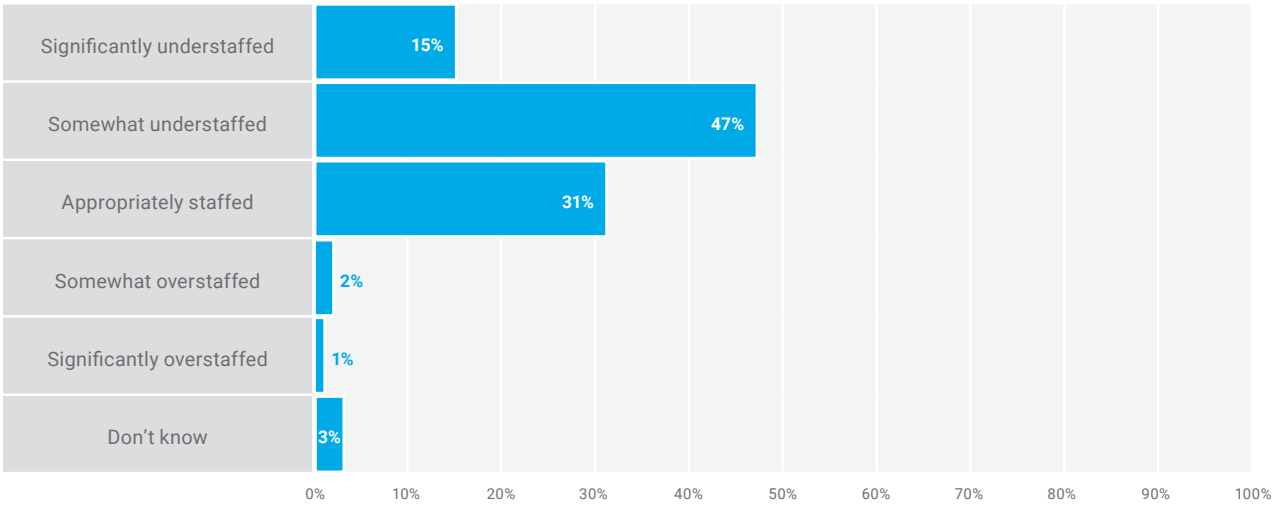
Challenges Persist in Cybersecurity Resourcing

The demand for cybersecurity talent[2] has steadily risen, which is good news for new and aspiring practitioners. Although this year's survey results on staffing are largely consistent with prior-year data, current data reveal a sizeable shift away from assessments of significantly understaffed to appropriately staffed (**figure 3**). Last year, 21 percent of respondents reported that their cybersecurity team was significantly understaffed; only 15 percent report the same perception this year. The percentage of respondents who believe that their cybersecurity team is appropriately staffed increased from 25 percent last year to 31 percent this year.

The industry remains a seller's market and, consequently, enterprises face resourcing and retention issues. Analysis of this year's responses confirms that understaffed organizations are significantly more likely to have retention issues. Additionally, understaffed teams are significantly more likely to have experienced more cyberattacks during the last year—a point supported by other cyberworkforce data.[3]

FIGURE 3—CYBERSECURITY STAFFING

How would you describe the current staffing of your organization's cybersecurity team?



2 (ISC)²® estimates a global shortage of 4.07 million cybersecurity staff, which represents a 26-percent increase from 2018. Fifty-one percent of respondents to the 2019 *(ISC)² Cybersecurity Workforce Study* "say their organization is at moderate or extreme risk due to cybersecurity staff shortage." See (ISC)², *(ISC)² Cybersecurity Workforce Study, 2019: Strategies for Building and Growing Strong Cybersecurity Teams*, www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=D087F6468B4991E-0BEFFC017BC1ADF59CD5A2EF7.

3 *Ibid.*

Vacancies

Fifty-seven percent of respondents claim to have unfilled cybersecurity positions (**figure 4**), which closely aligns with last year's data (58 percent).

The amount of time required to fill a cybersecurity position (**figure 5**) moved little this year—which is not surprising—given the industry's widespread reporting of insufficient candidates for an increasing number of current and future human resource needs.

FIGURE 4—UNFILLED POSITIONS

Does your organization have unfilled (open) cybersecurity positions?

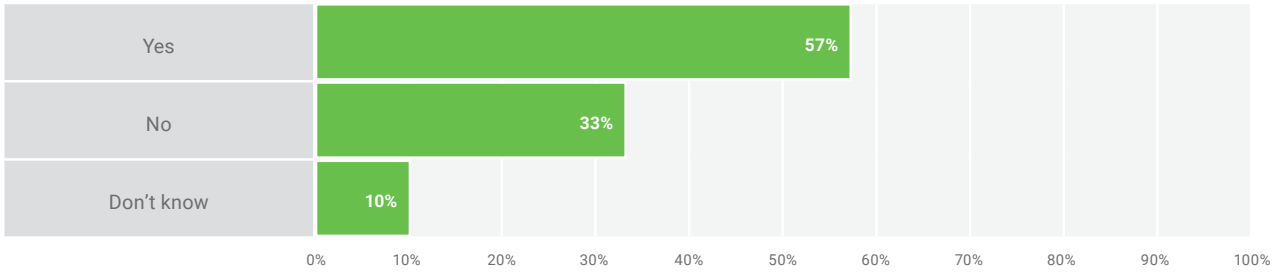
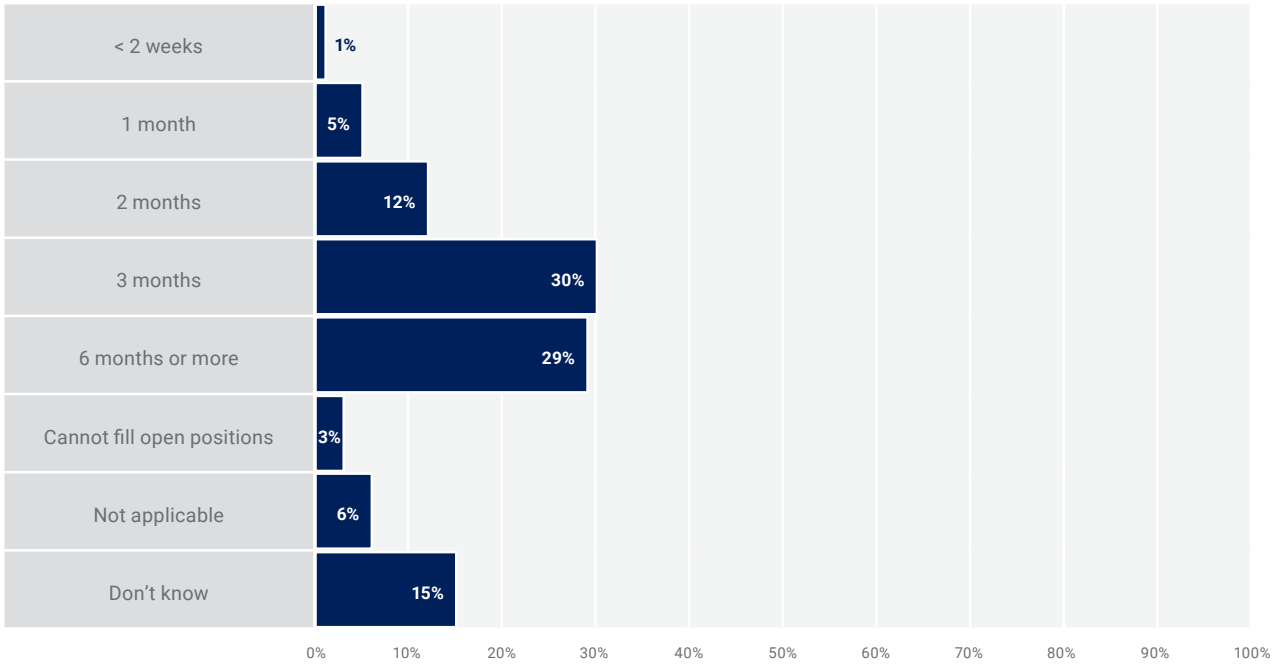


FIGURE 5—TIME TO FILL A CYBERSECURITY POSITION

On average, how long does it take your organization to fill a cybersecurity position with a qualified candidate?



Technical cybersecurity positions remained the top vacancy again this year (**figure 6**); however, all but executive-level positions declined from last year. **Figure 7** represents three-year reporting data regarding unfilled positions.

When asked about future demand (**figure 8**), respondents generally anticipate no change in the coming year, except for growth in individual contributor/technical cybersecurity positions (for which 78 percent expect increased demand). **Figure 9** charts three-year trends regarding future demand across various position categories.

FIGURE 6—PERCENTAGES OF UNFILLED POSITIONS AT GIVEN ORGANIZATIONAL LEVELS

How many of your unfilled (open) cybersecurity positions are at the following levels?

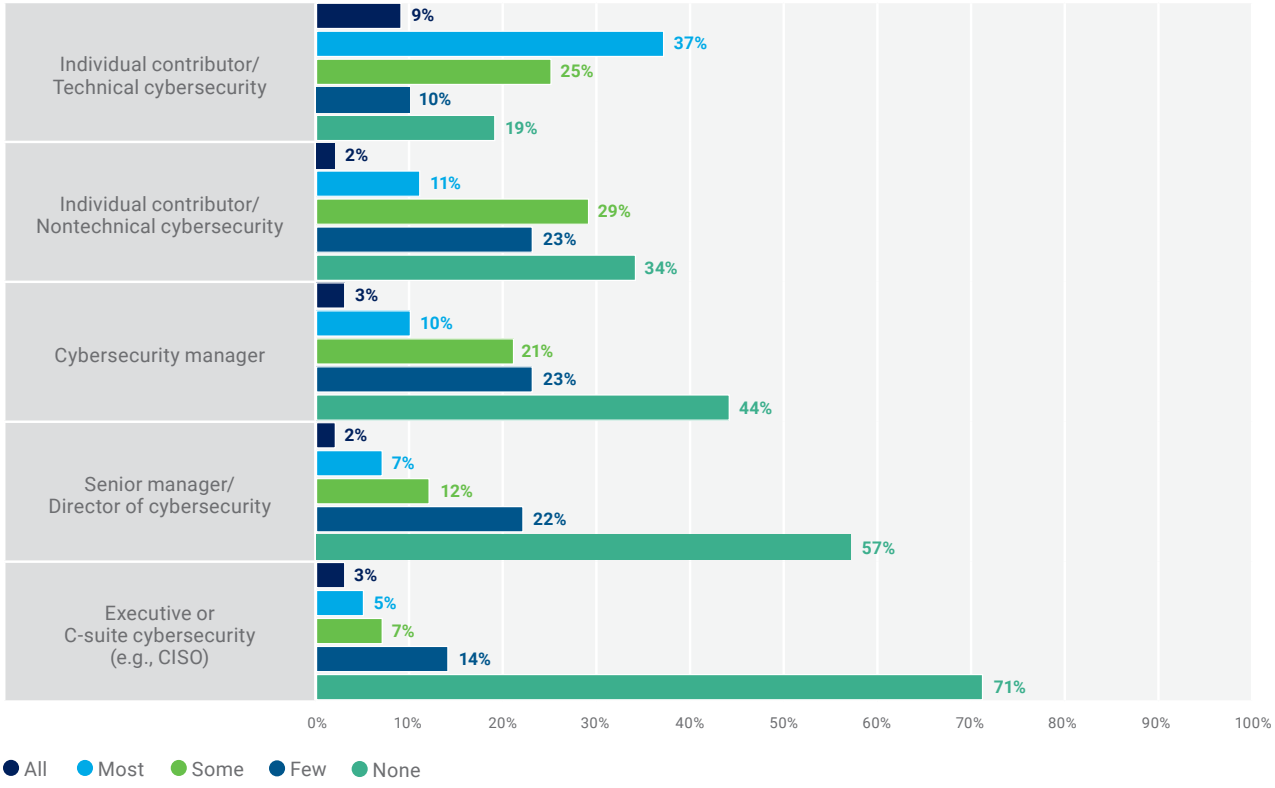


FIGURE 7—UNFILLED POSITION REPORTING (2018–2020)[4]

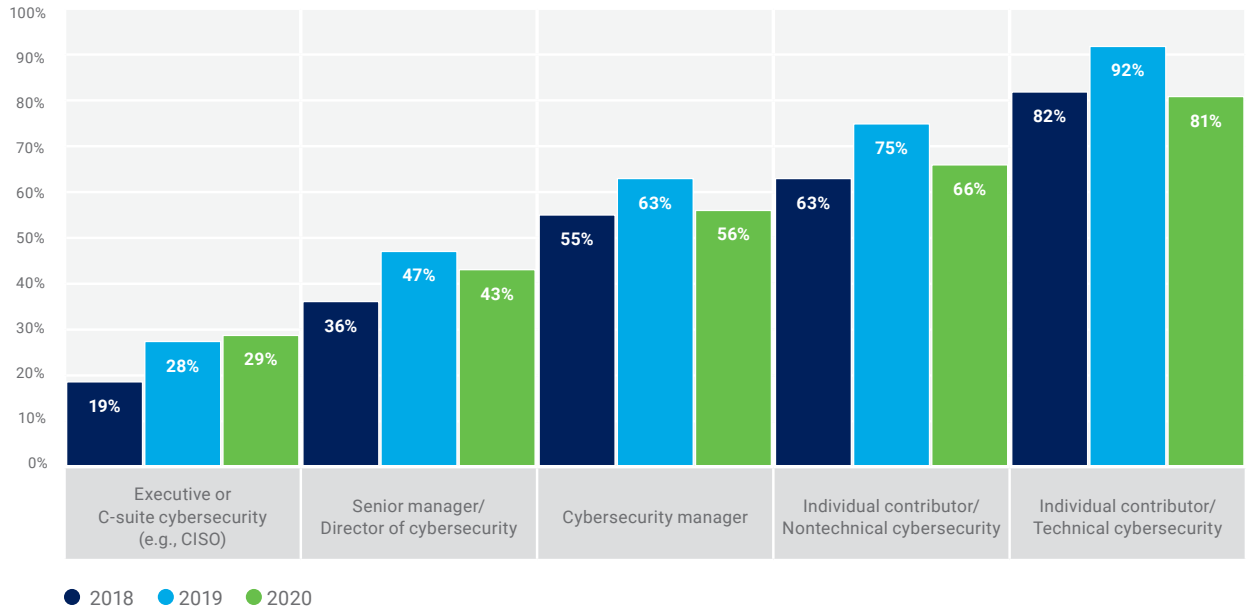
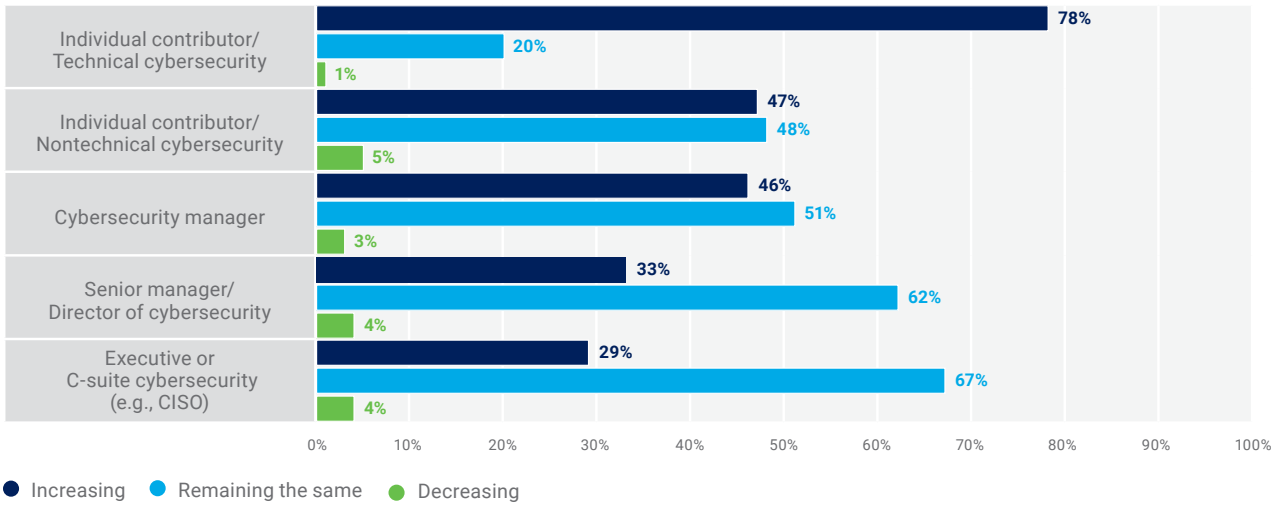


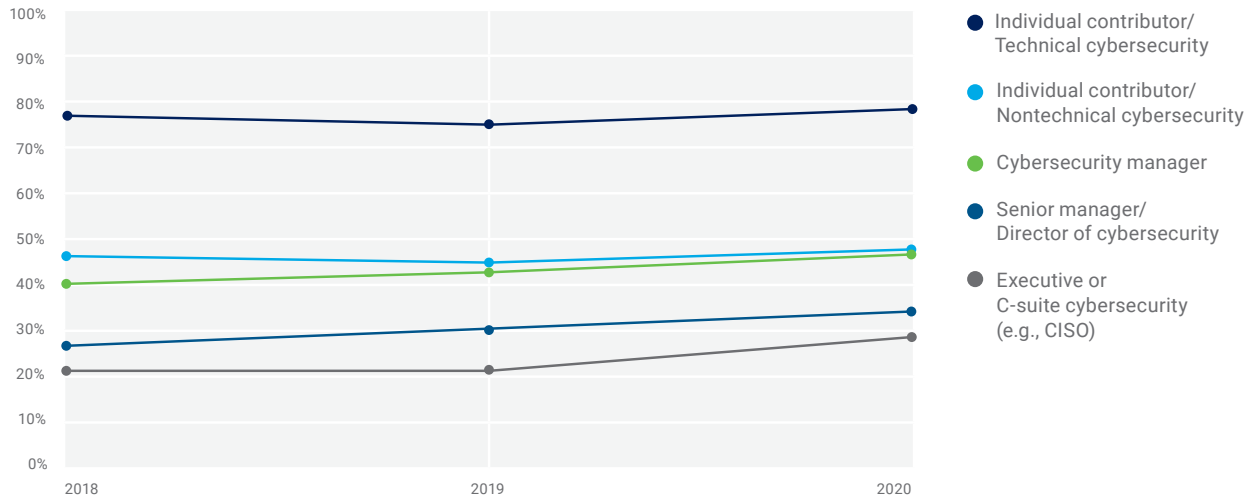
FIGURE 8—FUTURE HIRING DEMAND

In the next year, do you see the demand for the following cybersecurity position levels increasing, decreasing or remaining the same?



4 **Figure 7** compares unfilled position data aggregated from 2018–2020 *State of Cybersecurity* reports. Percentages represent all categories of vacancies less "none."

FIGURE 9—HIRING DEMAND TRENDING (2018–2020)

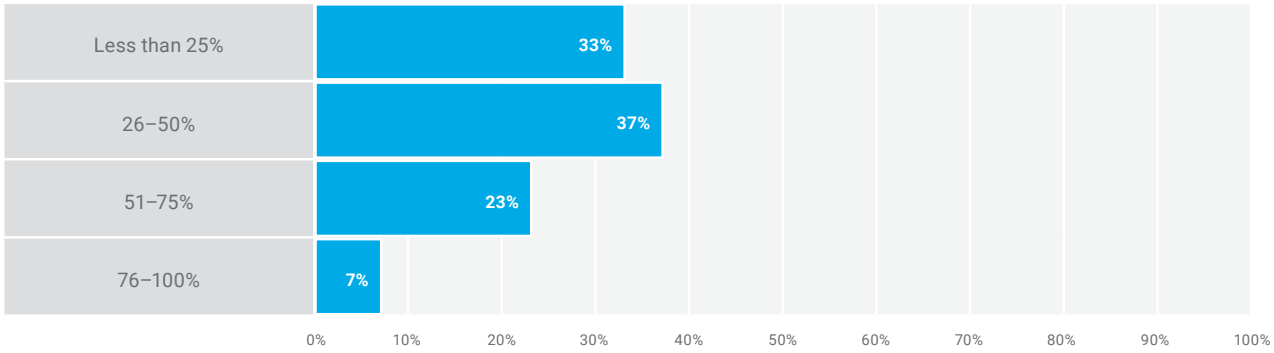


Qualifications and Confidence Levels

Survey results indicate that hiring manager confidence is low when it comes to applicants. **Figure 10** indicates that 70 percent of respondents generally do not believe their applicants are well qualified. Although this datapoint alone does not characterize deficiencies among applicants, it does help to explain delays in filling positions—not surprisingly, 73 percent of respondents who reported less than 25 percent of their applicants are well qualified have unfilled positions longer than three months.

FIGURE 10—PERCENTAGE OF CYBERSECURITY APPLICANTS WHO ARE WELL QUALIFIED

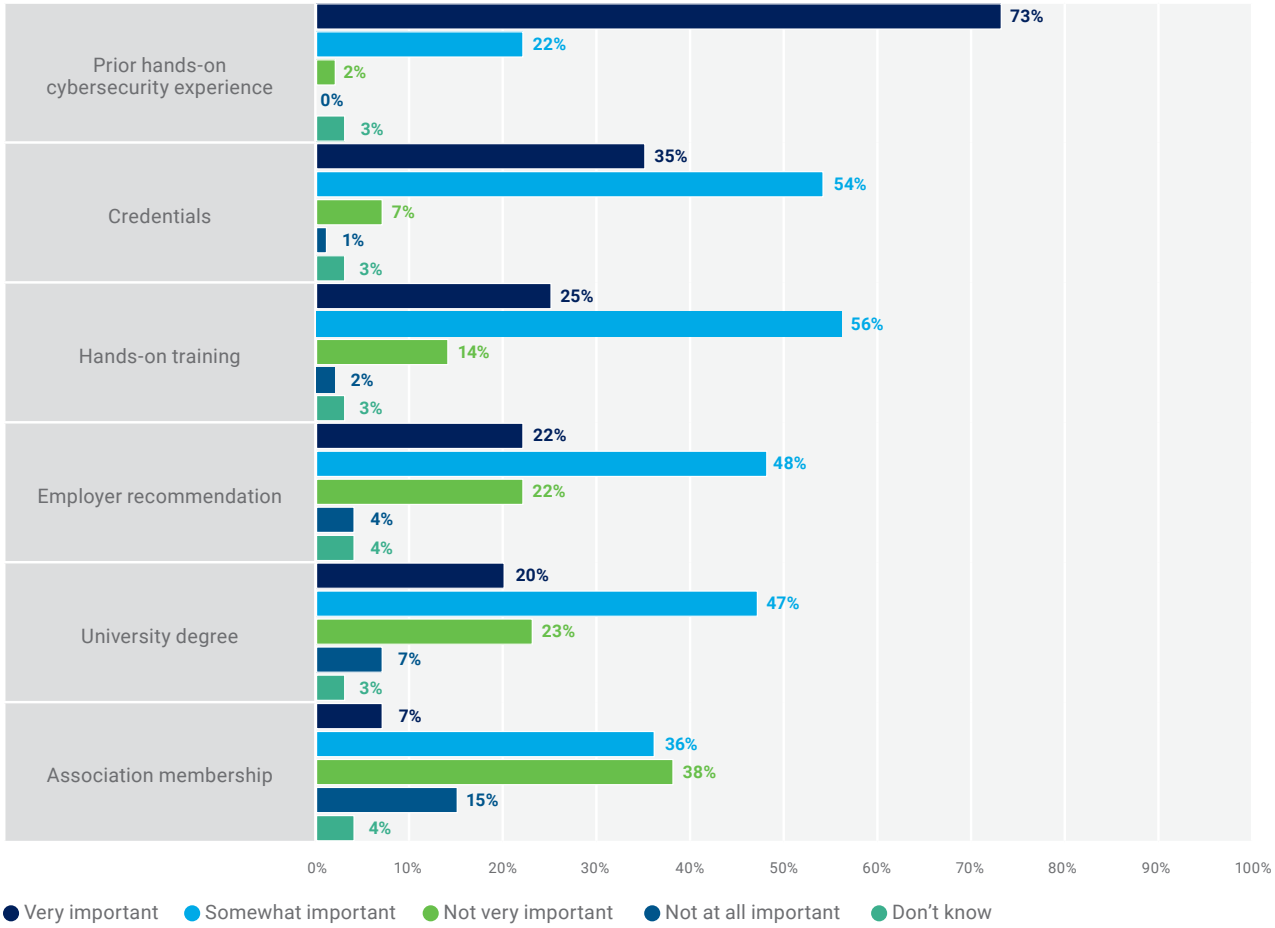
On average, how many cybersecurity applicants are well qualified for the position for which they are applying?



As shown in **figure 11**, prior hands-on cybersecurity experience remains the primary factor in determining whether a candidate is considered qualified. However, when asked about the largest skills gaps, the responses somewhat contradict this point. Respondents largely view soft skills as the primary gap among cybersecurity professionals (**figure 12**), followed closely by IT knowledge and skills gaps—specifically networking, infrastructure and IT operations. Respondents also indicate a lack of knowledge and/or experience with various technologies and applications as skills gaps.

FIGURE 11—CANDIDATE QUALIFICATIONS

How important are each of the following factors in determining if a cybersecurity candidate is qualified?



A deficit of soft skills may also be to blame in another area—recruitment. Survey data shown in **figure 13** illustrate a significant misunderstanding between hiring managers and those who identify and prescreen candidates. Seventy-two percent of respondents feel that their HR departments do not understand their needs.

Relatively higher degrees of understanding between hiring managers and HR departments correlate highly to filling open positions faster. Of those respondents who report that HR always fully understands their cybersecurity hiring needs, 29 percent hire in less than two months (which is quicker than most).

FIGURE 12—QUANTIFIED SKILLS GAPS[5]

What are the biggest skill gaps you see in today's cybersecurity professionals?

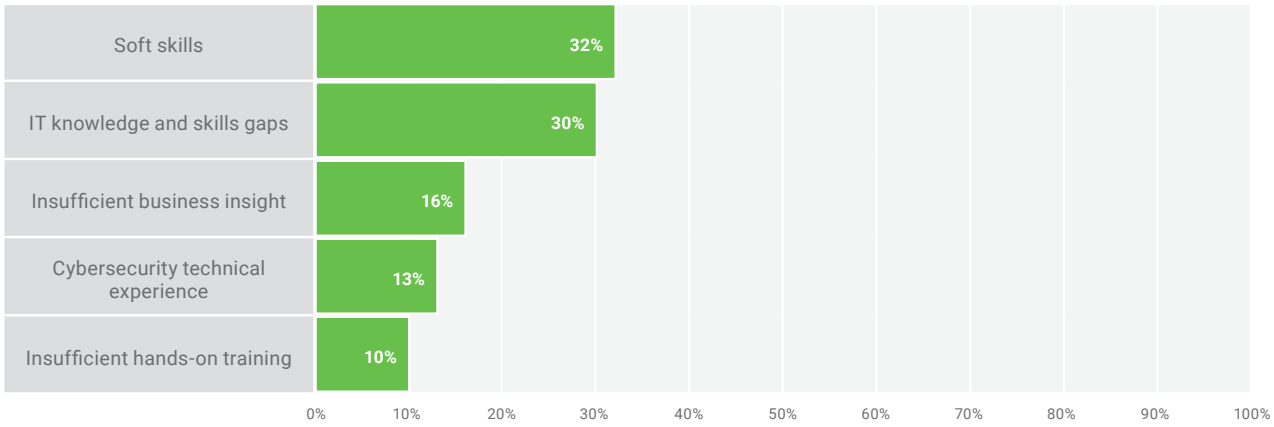
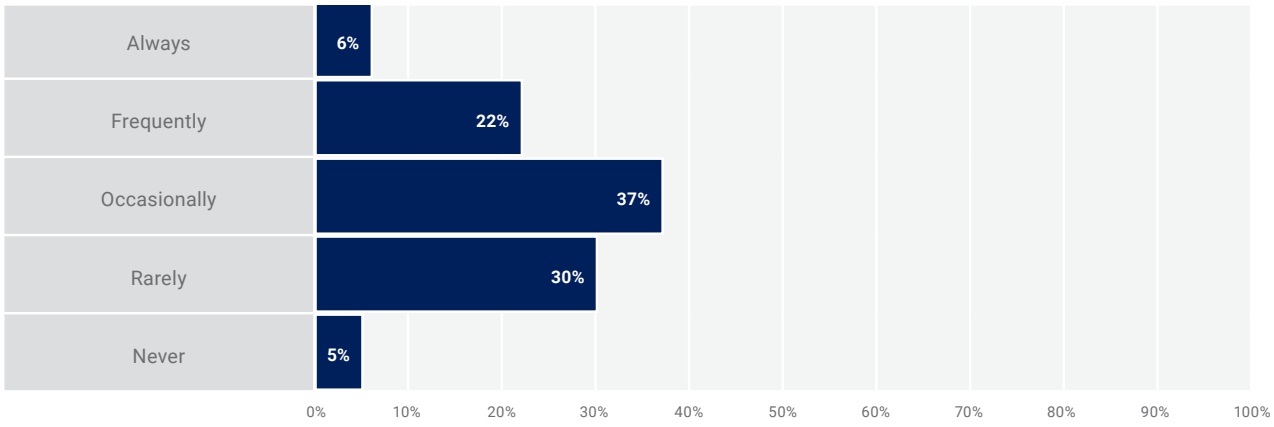


FIGURE 13—HR NEEDS COMPREHENSION

How often do you feel your HR department fully understands your cybersecurity hiring needs to properly prescreen candidates?



5 ISACA normalized and aggregated certain survey responses to clarify respondents' views on skills gaps. The aggregate category 'IT knowledge and skills gaps' in **figure 12** includes the following survey responses defining particular/discrete gaps: "different types of technologies and/or applications," "IT operations knowledge and skills" and "networking and/or other infrastructure knowledge and skills." The aggregate category 'Soft skills' combines the following discrete gaps: "insufficient soft skills" and "inability to collaborate between IT and the business units."

University Degree Programs Versus Training Programs

The cybersecurity talent gap continues to spur the growth of new organizations and programs that aim to develop—and/or increase—the candidate pool. There is no shortage of traditional academic programs and training courses in the market—each with certain advantages and disadvantages. Of the two, respondents regard hands-on training as more important than university degree programs (**figure 11**). Data represented in **figure 12** suggest, however, that neither security-specific degree programs nor training courses provide sufficient IT knowledge and skills for those just entering the cybersecurity profession.

Perceptions of university degrees in cybersecurity remain mixed among survey respondents. Forty-six percent report that they neither agree nor disagree that cybersecurity degrees prepare university graduates well for their future organizations' challenges (**figure 14**). This represents an eight percentage-point increase from a year ago. The percent of respondents who indicate that cybersecurity university degrees do not prepare graduates for today's challenges dropped to 28 percent this year, down from 39 percent last year. Despite this sentiment, 55 percent report that their organizations require a degree (**figure 15**), though responses vary by geography. For example, 78 percent of those responding from Africa indicate that their enterprises require a university degree to fill an entry-level cybersecurity

FIGURE 14—CONFIDENCE IN UNIVERSITY DEGREES

To what extent do you agree or disagree that recent university graduates in cybersecurity are well prepared for the cybersecurity challenges in your organization?

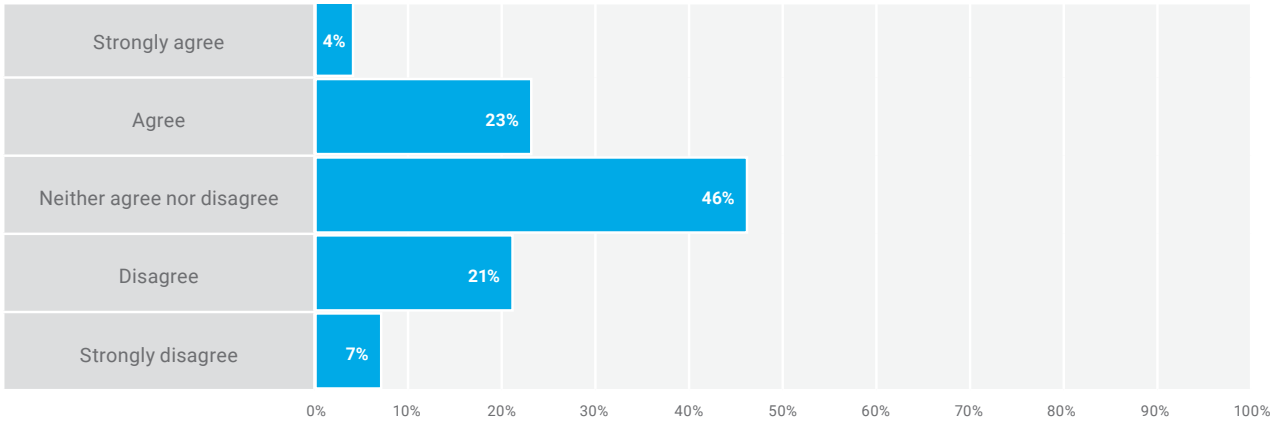
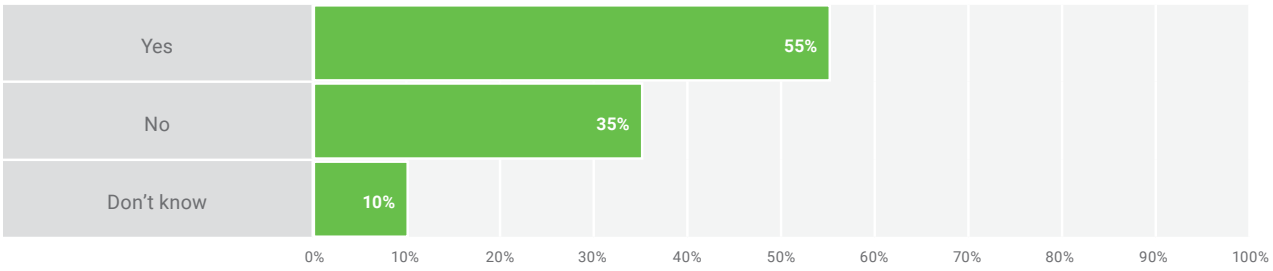


FIGURE 15—UNIVERSITY REQUIREMENT

Does your organization typically require a university degree to fill your entry-level cybersecurity positions?



position, while only 37 percent of those responding from Oceana indicate requiring a university degree. Respondents from other geographies fall somewhere in between regarding the university degree requirement—with Asia at 62 percent, Europe at 46 percent, Latin America at 64 percent, North America (including the Caribbean and Central America) at 54 percent and the Middle East at 67 percent.

Reporting shows that a large majority of cybersecurity professionals do have a degree. According to the *(ISC)² Cybersecurity Workforce Study, 2019*, 88 percent of practitioners have a degree—most at the bachelor-degree level or higher.[6] The value of formal education is beyond the scope of this paper and arguably varies by region. However, given the cybersecurity human capital crisis that threatens global markets—and, when it comes to personal privacy, for example, jeopardizes the reputations of everyday citizens, or even continuity of life in hospitals or other healthcare settings—it becomes clear that not only enterprises, but the public in general, would benefit from greater numbers of cybersecurity applicants. Mandating degrees—especially via automated recruiting platforms—unnecessarily constrains talent pools.

Retention Remains A Challenge

This year, 66 percent of survey respondents indicate difficulty retaining talent—a slight increase over last year's 64 percent. Although justification varies, respondents overwhelmingly feel that cybersecurity professionals leave positions because they are actively recruited (**figure 16**). Like last year, respondents ranked limited promotion and development opportunities as a likely reason for professionals to leave current jobs. The data further indicate that people leave positions not just on account of financial reasons—an encouraging result for enterprises with strained budgets. Forty percent of respondents attribute departures to workplace stress, which marks a 10 percentage-point increase over the year prior. Not surprisingly, organizations with unfilled cybersecurity positions are significantly more likely also to have retention issues.

Enterprises recognize that there is no quick answer to their cybersecurity-resource woes. Accordingly, they continue to address their respective skills gaps this year (**figure 17**)—although different mitigation strategies surface more prominently in current-year results, compared to prior year. Cross-training of organizational personnel and increased use of contractors and consultants are the primary mitigations of survey respondents. Thirty percent of enterprises report using artificial intelligence (AI) in their security operations, which may explain the slight uptick in the reported use of AI or automation to mitigate skills gaps. ISACA expects this implementation of AI to trend higher as strategies and solutions are increasingly proven beneficial within various industries.

Performance-based training and requiring credentials—although viable and beneficial—do not uniformly mitigate skills gaps, nor do they decrease the workplace stress that accompanies shorthanded teams.

6 *Op cit* (ISC)²

FIGURE 16—WHY CYBERSECURITY PROFESSIONALS LEAVE THEIR JOBS

Which, if any, of the following factors do you feel are causing cybersecurity professionals to leave their current jobs? Select the top 5 factors.

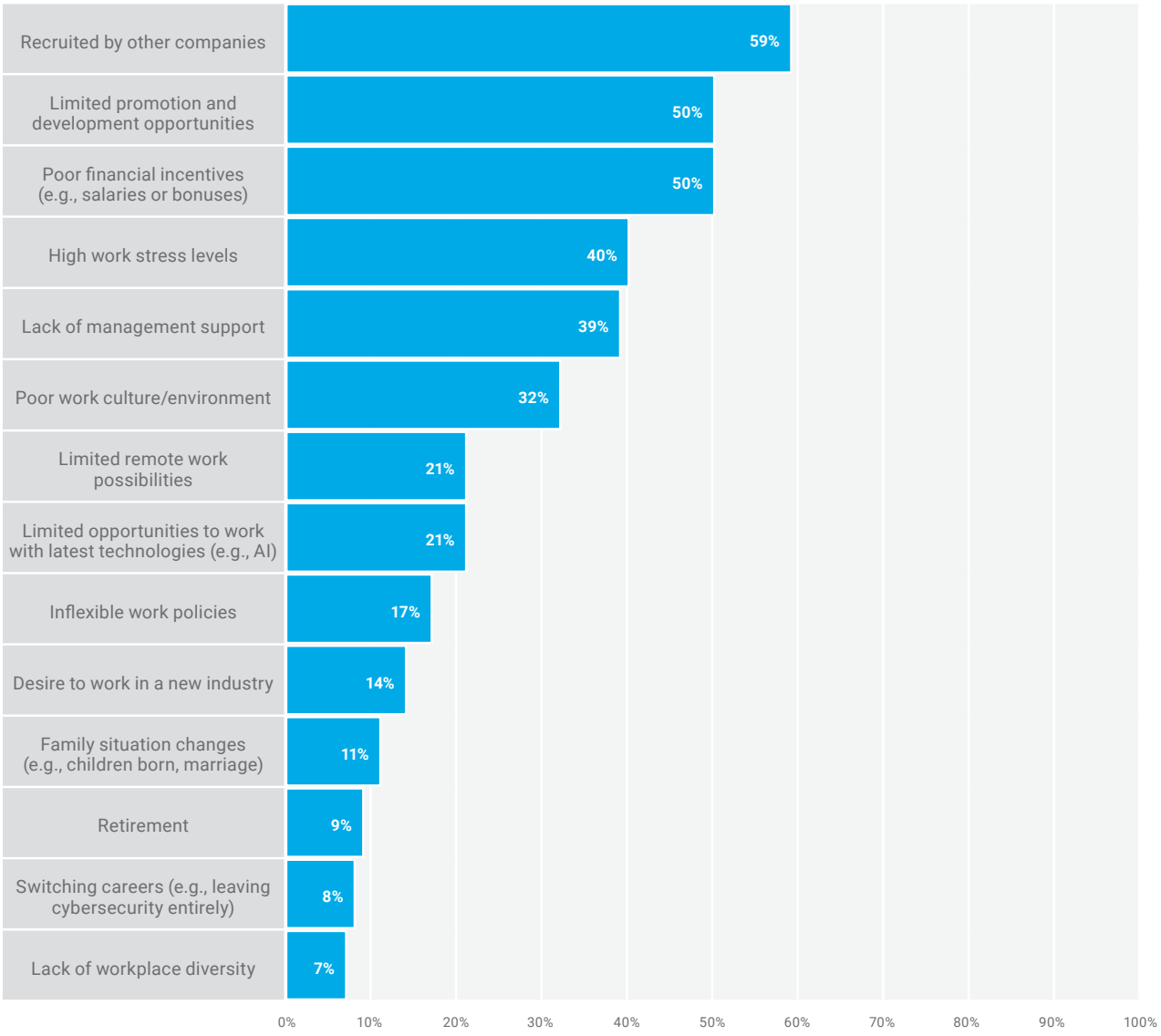
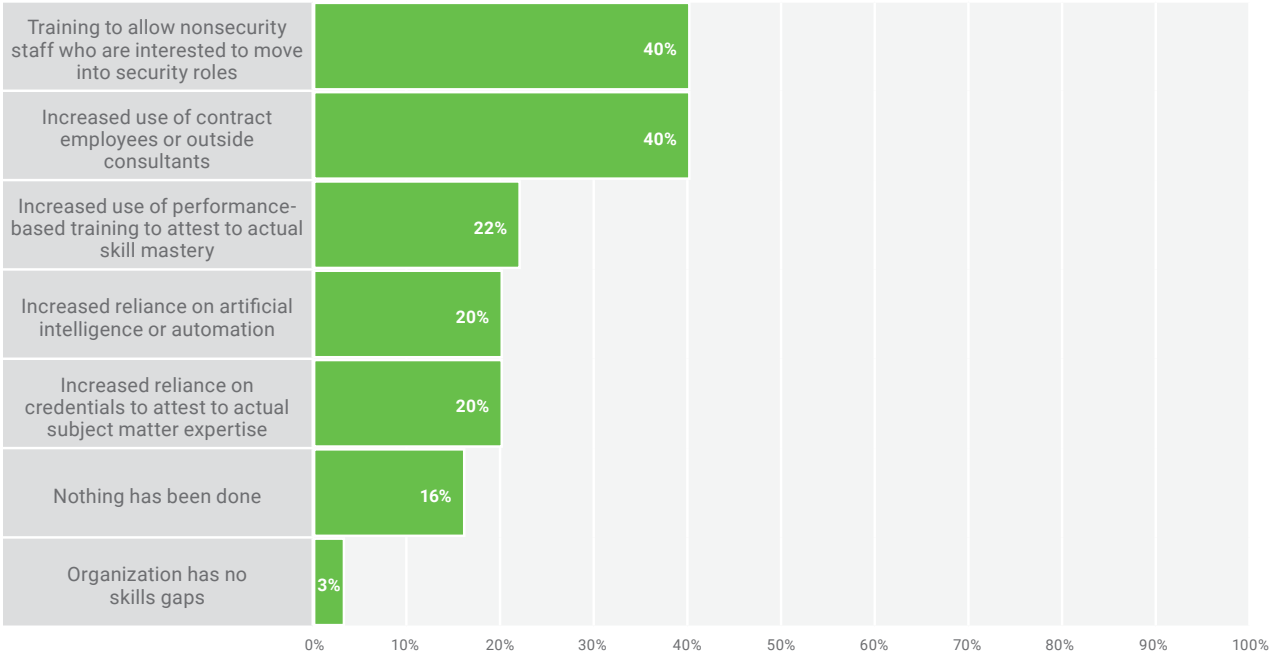


FIGURE 17—MEANS OF MITIGATING SHORTFALLS

Which, if any, of the following has your organization undertaken to help decrease the perceived cybersecurity skills gaps? Select all that apply.



Gender Diversity Within Cybersecurity—Slow but Steady Improvement

Gender Diversity and Disparity

Overall, this year's survey results extend the last two years' reporting of a male-dominated workforce: Eighty-six percent of recent respondents report the employment of more men than women in their enterprises' security roles (**figure 18**). However, this figure represents a small decrease (three percentage points) from last year, while the number of respondents indicating equal numbers of men and women increased three percentage points.

Most respondents believe that women are afforded the same opportunities for career advancement as men—81 percent—up one percentage point from the prior year (**figure 19**). The number of women who believe that they are afforded the same opportunities as men increased 6 percentage points (to 51 percent), and the gap between the numbers of men and women who perceive equal opportunity for career advancement narrowed by 7 percentage points from a year ago.

Forty-seven percent of respondents indicate that their enterprise has a goal to increase the number of women in cybersecurity roles—a two-percentage point gain from last year; the number of women making that claim increased five percentage points to 38 percent.

FIGURE 18—PROPORTION OF MEN VS. WOMEN IN CYBERSECURITY ROLES

How would you describe the current proportion of men versus women in cybersecurity roles in your organization?

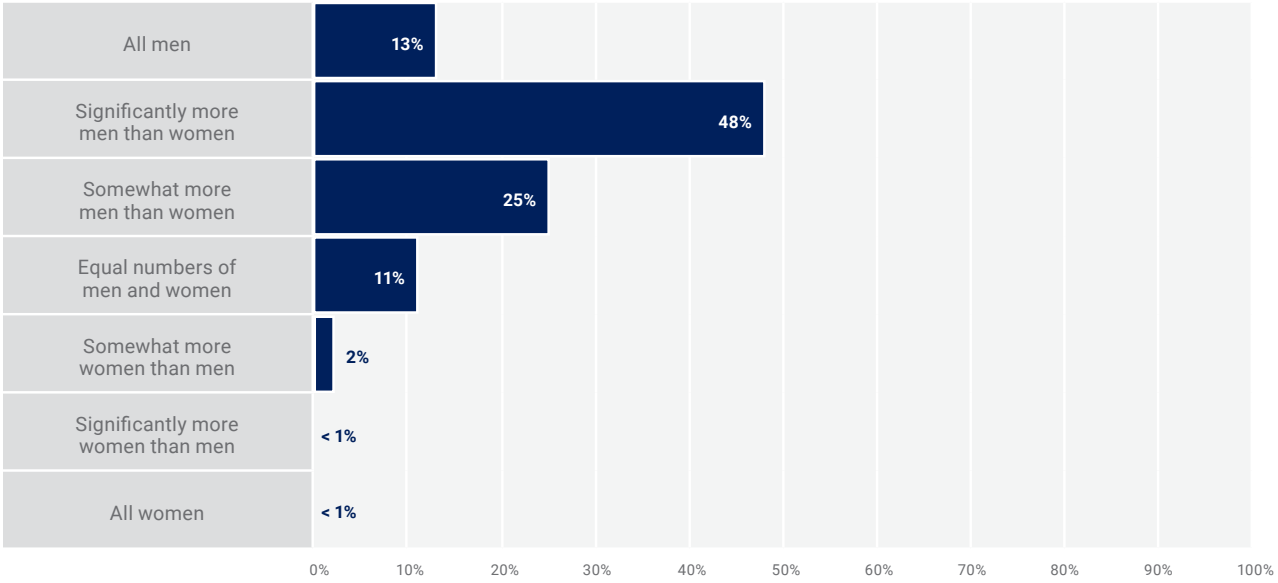
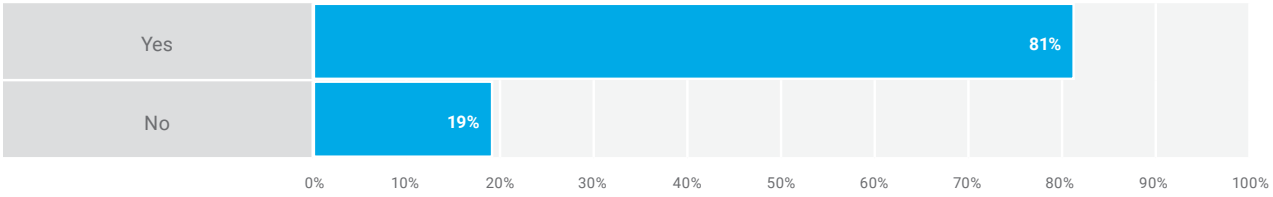


FIGURE 19—GENDER DISPARITY

Do you believe that women are offered the same opportunities for career advancement as men are offered in the field of cybersecurity in your organization?



Gender Initiatives

Despite an increasing number of global initiatives to boost the number of women in technology careers, expectations should be tempered as broad-scale workforce efforts take time to cultivate. That said, 64 percent of those surveyed indicate some progress—however slight—towards increasing the number of women in cybersecurity roles (**figure 20**). The positive changes in this year's data are promising. According to the data, almost half of all enterprises—49 percent—have gender diversity programs in place, which is five percentage points higher than last year (**figure 21**).

FIGURE 20—ORGANIZATIONAL PROGRESS TOWARD INCREASING WOMEN IN CYBER ROLES

How would you describe the progress that your organization has made in increasing the number of women in cybersecurity roles?

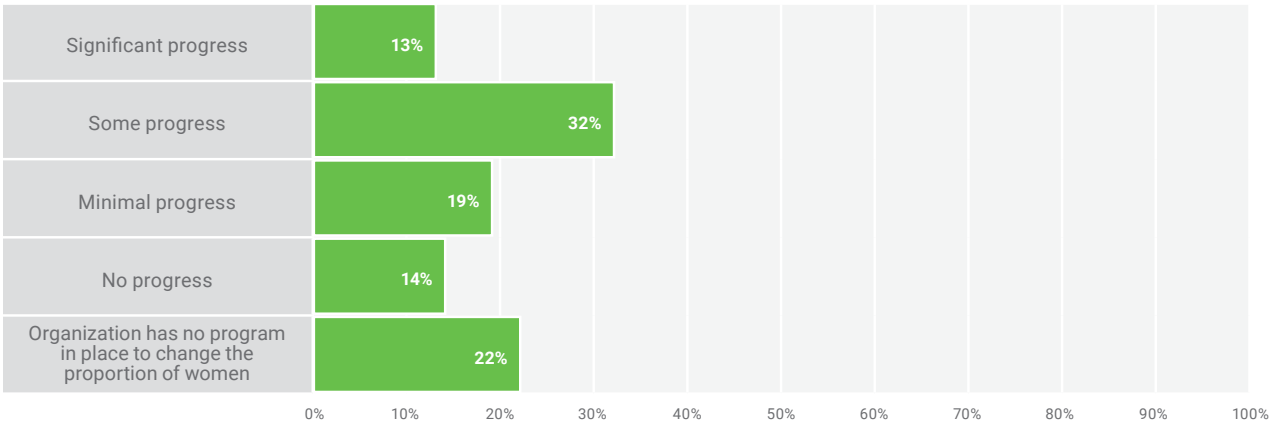
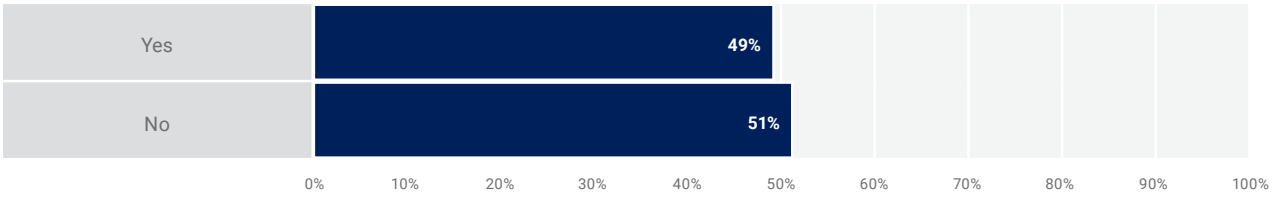


FIGURE 21—DIVERSITY PROGRAMS

Does your organization have in place specific diversity programs to support women cybersecurity professionals?



Signs of Leveling in Cybersecurity Funding

Cybersecurity budgets are projected to bounce back in 2020; however, the increase remains less than the 64 percent reported two years ago.[7] Specifically, 58 percent of respondents anticipate an increase in cybersecurity budgets (**figure 22**), which is an increase of three percentage points from last year. This increase is notable because the data in **figures 22** and **23** suggest spending may be leveling out, given the five-year trend represented in **figure 24**.

FIGURE 22—ENTERPRISE SECURITY BUDGET OUTLOOK

How, if any, will your organization's cybersecurity budget change in the next 12 months?

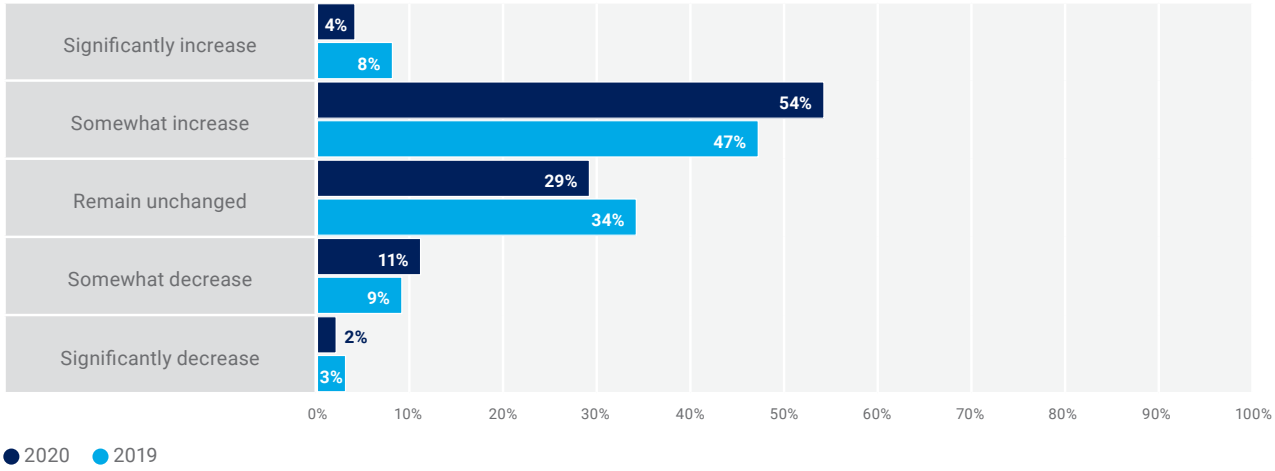
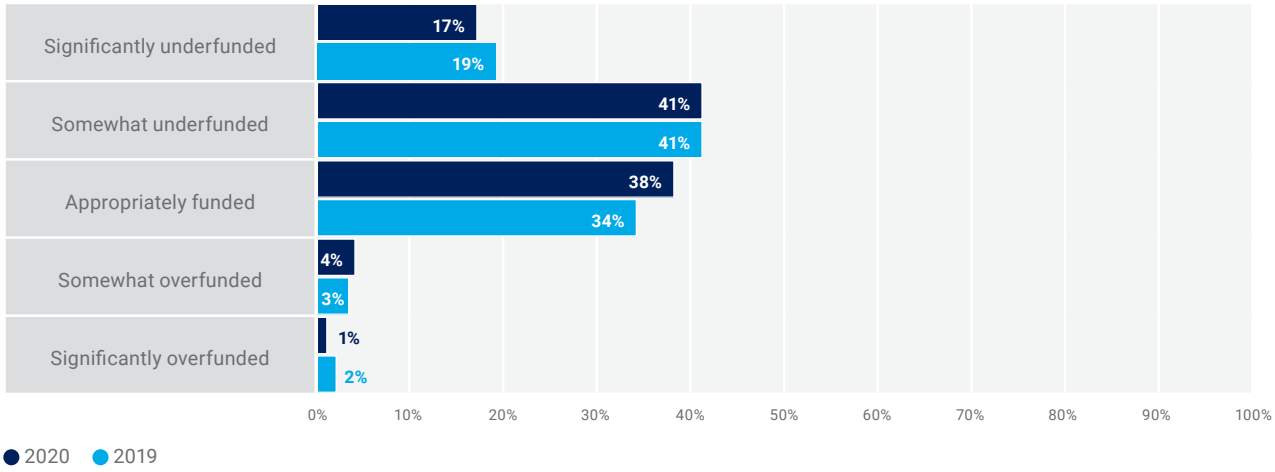


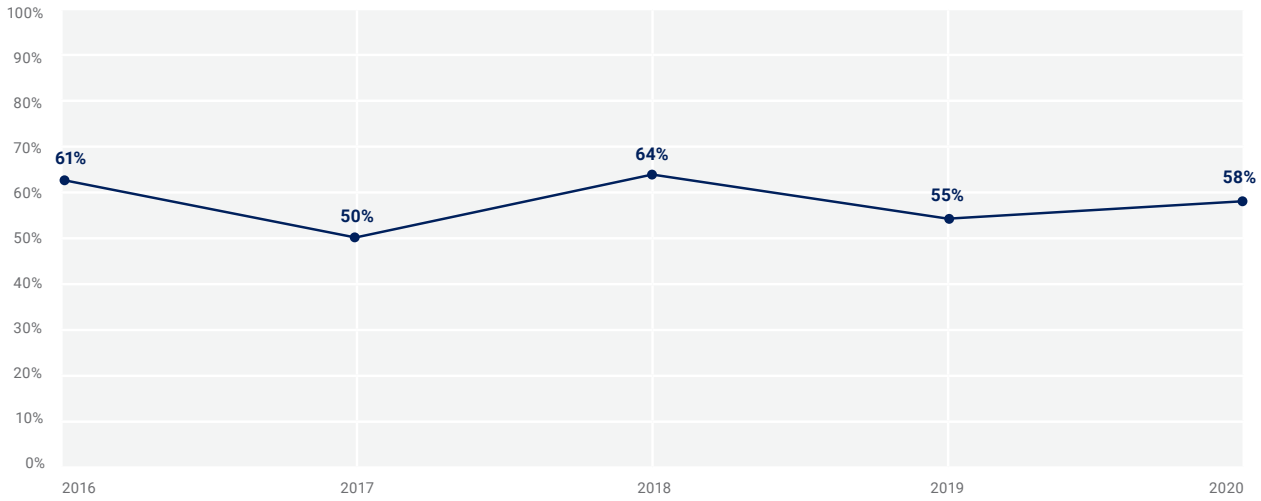
FIGURE 23—CYBERSECURITY FUNDING PERCEPTION

Do you feel your organization's cybersecurity budget is currently…



7 ISACA, *State of Cybersecurity 2018, Part 1: Workforce Development*, https://cybersecurity.isaca.org/csx-resources/state-of-cybersecurity-2018

FIGURE 24—FORECASTED SECURITY BUDGET INCREASES (5 YEAR)



Conclusion: Organizations Must Act on Talent Shortage

The cybersecurity workforce shortage is not new, nor is it going away soon. Formal educational programs and industry cybersecurity training programs—despite their proliferation—cannot replicate cybersecurity experience, which is the most sought-after criterion for filling a vacant job position. Organizations have difficulty locating individuals with the desired experience, and increasingly poach qualified talent from other enterprises—a practice whose frequency is likely to increase. The excessive time required to fill open positions not only exacerbates workplace stress but is also associated with increased cyberattacks and retention issues.

Most organizations have experienced a bad hire, which can prove undesirable and costly in some instances. However, that risk pales in comparison to any recently documented cybersecurity incident. With so few qualified applicants, organizations are wise to cross-train existing employees. Investing in familiar, motivated individuals—who already understand the organization's business drivers and culture—can help to satisfy some of the knowledge and skills gaps reported in this year's survey. Gender diversity programs are one vehicle to increase organizational talent, but they cannot be the only solution to combat the talent shortage. More can be done, but it requires commitment and nontraditional recruiting. Formal education and industry training programs can be cost prohibitive for many aspiring practitioners. Mandating college degrees and certifications minimizes talent pools and disadvantages those who could not afford to fulfill traditional requirements for cybersecurity jobs. Government workforce development or employment agencies may also be viable sources for displaced workers or career changers. The cybersecurity seller's job market will not diminish anytime soon; with budgets leveling out—and retention waning—traditional recruitment strategies may have to give way to new and inventive alternatives.

Acknowledgments

ISACA would like to recognize:

ISACA Board of Directors

Brennan P. Baybeck, Chair
CISA, CRISC, CISM, CISSP
Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

Rolf von Roessing, Vice-Chair
CISA, CISM, CGEIT, CISSP, FBCI
FORFA Consulting AG, Switzerland

Tracey Dedrick
Former Chief Risk Officer with Hudson City Bancorp, USA

Pam Nigro
CISA, CRISC, CGEIT, CRMA
Health Care Service Corporation, USA

R.V. Raghu
CISA, CRISC
Versatilist Consulting India Pvt. Ltd., India

Gabriela Reynaga
CISA, CRISC, COBIT 5 Foundation, GRCP
Holistics GRC, Mexico

Gregory Touhill
CISM, CISSP
AppGate Federal Group, USA

Asaf Weisberg
CISA, CRISC, CISM, CGEIT
introSight Ltd., Israel

Rob Clyde
ISACA Board Chair, 2018-2019
CISM
Board Director, Titus and Executive Chair, White Cloud Security, USA

Chris K. Dimitriadis, Ph.D.
ISACA Board Chair, 2015-2017
CISA, CRISC, CISM
INTRALOT, Greece

Greg Grocholski
ISACA Board Chair, 2012-2013
CISA
Saudi Basic Industries Corporation, USA

David Samuelson
Chief Executive Officer, ISACA, USA

About ISACA

For more than 50 years, ISACA® (www.isaca.org) has advanced the best talent, expertise and learning in technology. ISACA equips individuals with knowledge, credentials, education and community to progress their careers and transform their organizations, and enables enterprises to train and build quality teams. ISACA is a global professional association and learning organization that leverages the expertise of its 145,000 members who work in information security, governance, assurance, risk and privacy to drive innovation through technology. It has a presence in 188 countries, including more than 220 chapters worldwide.

Disclaimer

ISACA has designed and created *State of Cybersecurity 2020, Part 1: Global Update on Workforce Efforts and Resources* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

ISACA

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Web: www.isaca.org

Provide feedback:
www.isaca.org/state-of-cybersecurity-2020

Participate in the ISACA Knowledge Center:
www.isaca.org/knowledge-center

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAGlobal

Instagram:
www.instagram.com/isacanews/