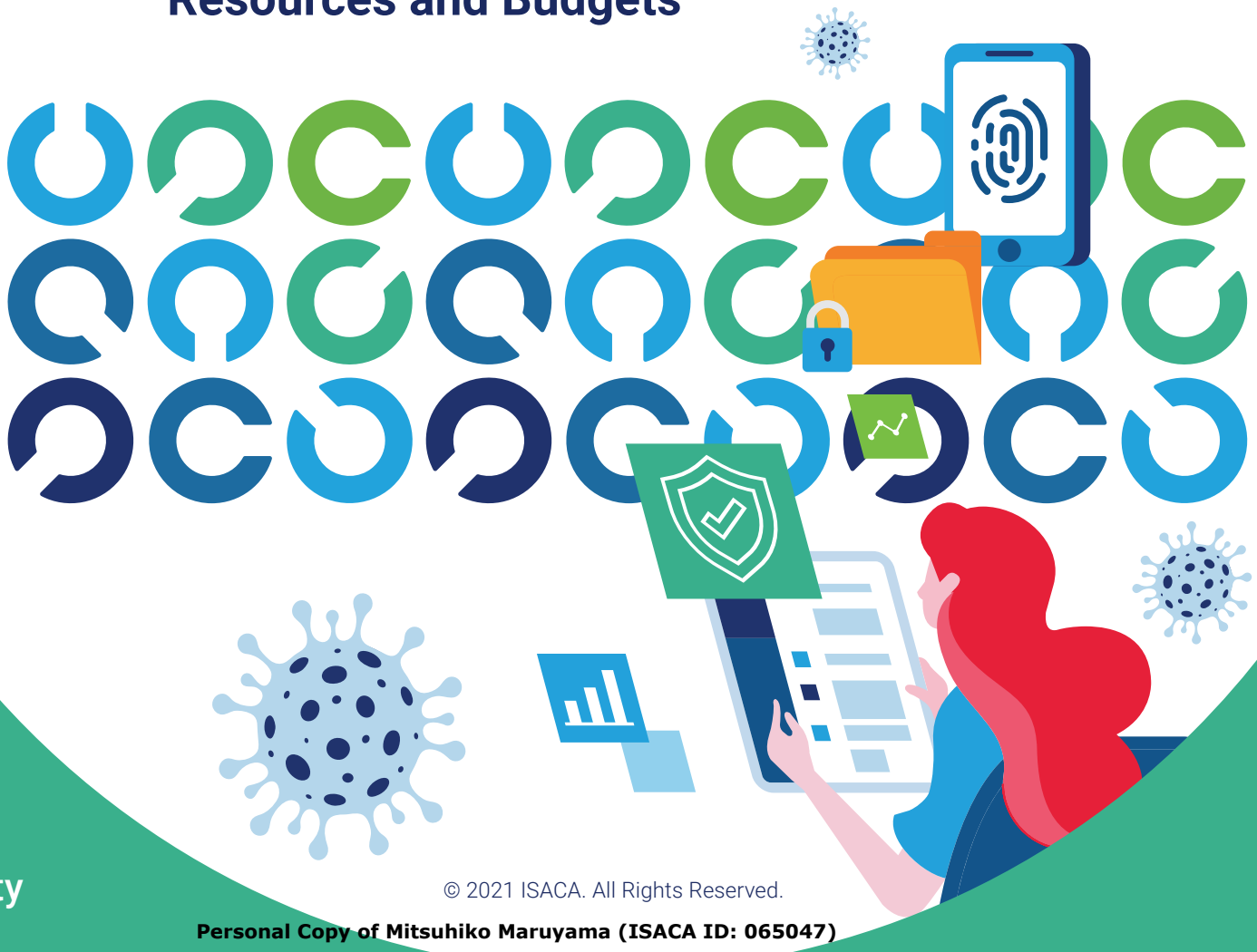
State of Cybersecurity 2021

Part 1: Global Update on Workforce Efforts, Resources and Budgets



Security

CONTENTS

ABSTRACT

State of Cybersecurity 2021, Part 1: Global Update on Workforce Efforts, Resources and Budgets reports the results of the annual ISACA® global *State of Cybersecurity Survey,* conducted in the fourth quarter of 2020. This Part 1 report focuses on the current trends in cybersecurity workforce development, staffing and cybersecurity budgets. The survey findings reinforce past reporting and, in certain instances, mirror prior year data despite enterprises dealing with a global pandemic and the resulting resource and finance issues. Staffing levels, ease of hiring, and retention remain pain points across the globe, and cybersecurity budgets continue a downward trend.

The issue of cybersecurity workforce deficiencies remains unresolved, despite years of reporting on this problem from numerous resources. This report features expert commentary from government officials, industry representatives and apprenticeship advocates to help enterprises understand the problem and to provide possible solutions.

Executive Summary

Now in its seventh year, the ISACA® global *State of Cybersecurity Survey* continues to identify current challenges and trends in the cybersecurity field. *State of Cybersecurity 2021, Part 1* analyzes the current survey results regarding cybersecurity workforce development and resourcing. In Part 2 of this report, ISACA examines the survey results relating to IT-related operations, cyberthreats and cybermaturity.

The survey findings are largely consistent with the findings from prior years: Enterprises continue to lack desired staffing levels to combat cyberthreats. Although the impact of COVID-19 on many businesses and enterprises is negative, respondent data show that the global pandemic helps retention. However, hiring talent remains challenging. Also, optimism surrounding cybersecurity budgets continues to slide despite a sizable number of respondents reporting pandemic-specific security spending.

ISACA and many others have been reporting cybersecurity workforce shortages that have not improved significantly in over five years. This report features expert commentary from industry participants, governmental bodies and apprenticeship programs to help enterprises understand why the workforce shortage is not lessening—at least to a certain degree. Much work remains to be done to improve the workforce pipeline, but the good news is that many organizations are tackling the problem.

Lack of equity and diversity are global issues plaguing all technology-related fields. In 2020, ISACA launched the One In Tech™ foundation, which seeks to build a healthy digital world that is safe, secure and accessible for all. To aid the One In Tech strategic evidence-based initiatives, ISACA transferred all diversity-related data collection to the foundation. Thus, unlike reports released in prior years, *State of Cybersecurity 2021* does not address diversity issues.[1]

Survey Methodology

In the final quarter of 2020, ISACA sent online survey invitations to a global population of cybersecurity professionals who hold the ISACA Certified Information Security Manager® (CISM®) certification or have registered information security job titles. The survey data were collected anonymously via SurveyMonkey. A total of 3,659 respondents completed the survey in its entirety, and their responses are included in the results.[2]

The survey, which used multiple-choice and Likert-scale formats, was organized into five major sections:

- Hiring and skills
- Security operations
- Cybersecurity budgets
- Cyberattacks and threats
- Organizational governance and risk management

The survey target population includes individuals who have cybersecurity job responsibilities. Of the 3,659 respondents, 1,721 indicate that cybersecurity is their primary professional area of responsibility. **Figure 1** shows demographic information about the respondents, who hail from over 120 countries. **Figure 2** further illustrates the breadth of survey input, showing that respondents represent more than 17 industries.

[1] ISACA continues to focus on diversity issues, but these issues span much more than the cybersecurity space. One In Tech, an ISACA Foundation founded in 2020, is now better able to investigate and communicate findings on these important issues.
[2] 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, consistent with prior-year survey reports. Result percentages are rounded to the nearest integer.

FIGURE 1: Respondent Demographics

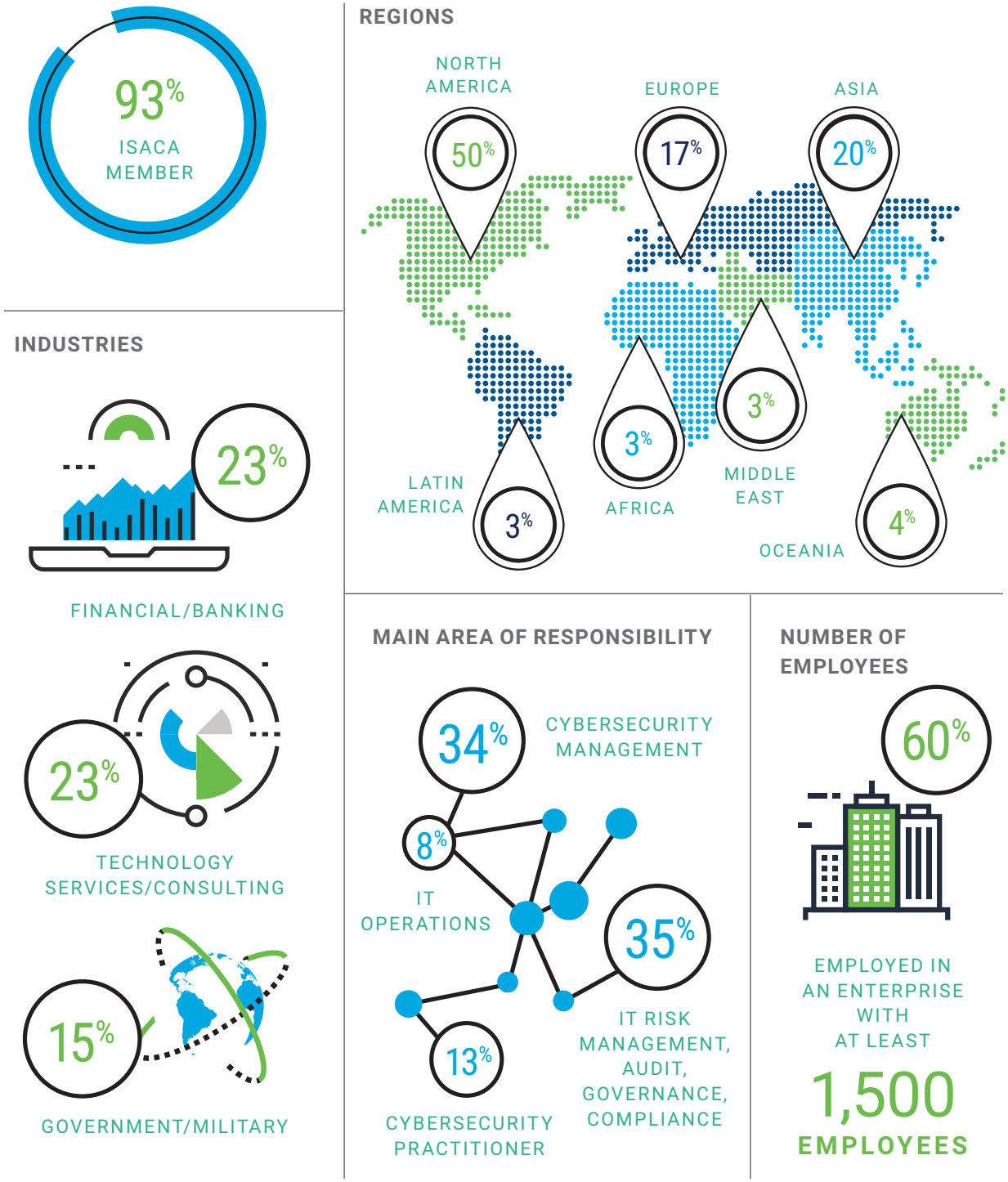
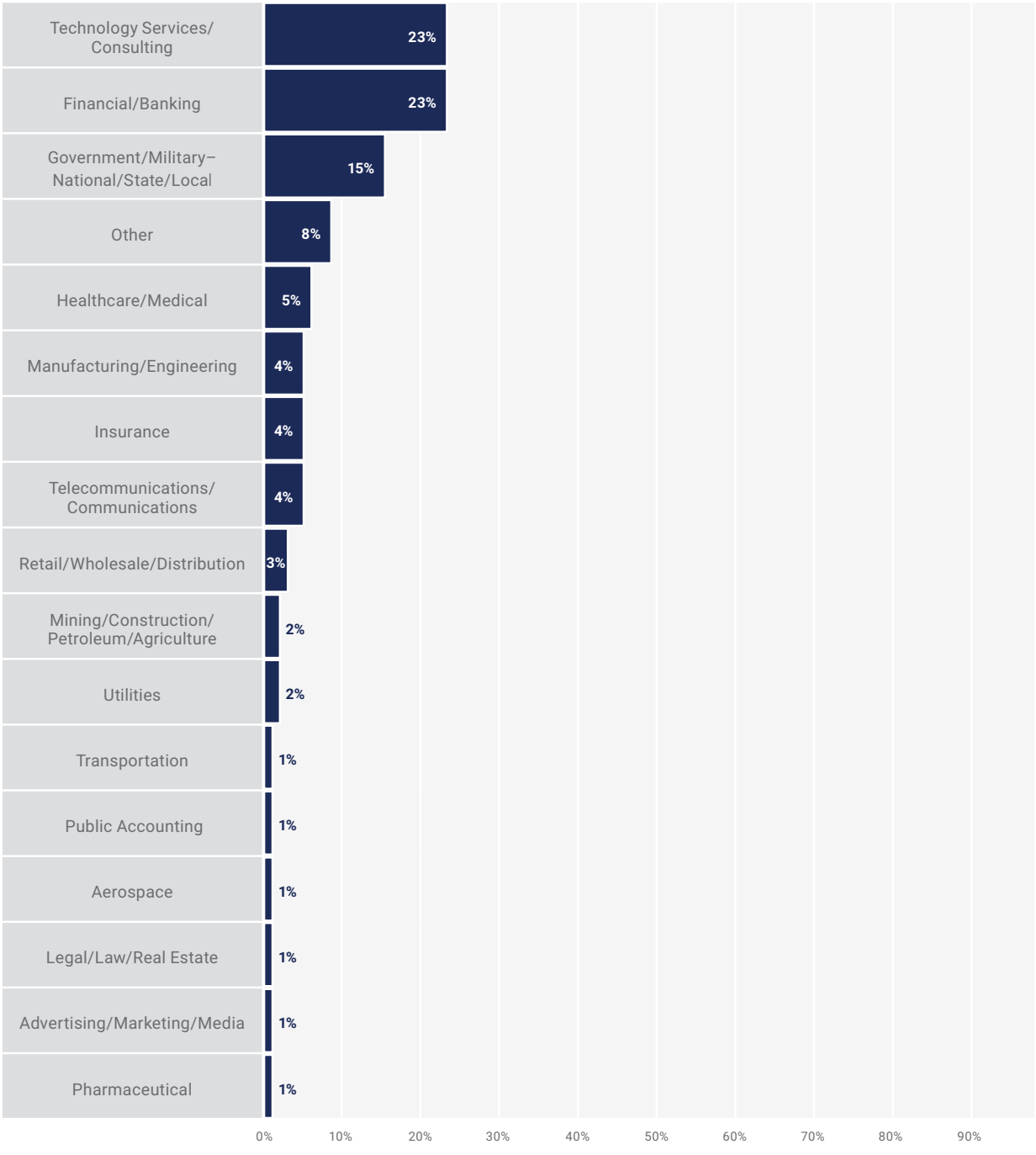


FIGURE 2: Industries Represented

Please indicate your organization's primary industry.



Uncertainty Amid a Global Pandemic

For a multitude of enterprises in 2020, the global COVID-19 pandemic required business leaders to think and execute differently. Business leaders who once balked at remote work had to change their mindset or risk financial ruin. Although not every industry or occupation is conducive to remote work, the pandemic is proving that a great deal of work can be performed outside the traditional office—often with little impact on business. Some enterprises are pleasantly discovering an increase in productivity while employees work remotely during the pandemic, which may forever sunset business-as-usual mindsets that have long bolstered exorbitant travel budgets and expansive capital expenditures.

Business leaders who once balked at remote work had to change their mindset or risk financial ruin.

Business survival favors the prepared, and industry reporting suggests that the cybersecurity profession—albeit understaffed and overworked—rose to the occasion, enabling enterprises across the globe to pivot very quickly to a wholly or mostly remote workforce.[3]

Because 2020 was anything but typical, readers are cautioned against interpreting any sizable shifts in workforce estimates during this period. Location and government mandates highly influenced which work was permissible and how that work was to be done. Government responses to the pandemic varied by country, region and locality.[4, 5] For example, many businesses in North America—especially small to medium enterprises—were deemed nonessential and unable to conduct business fully. Similarly, pandemic response plans shuttered some industries, such as service and tourism. Enterprises that were permitted to remain open may have been susceptible to hiring freezes and other budgetary impacts to keep the lights on and minimize financial loss. Reports of work reductions and salary cuts in the cybersecurity industry show that it was not immune to business operational adjustments.[6]

The demand for cybersecurity talent has risen steadily for years, which is promising for aspiring practitioners and career changers. Unfortunately, workforce priorities often allow few entry-level positions for those without experience.

This year's survey findings on staffing-related issues nearly mirror those of last year, except for a slight three percentage-point increase in those who report being appropriately staffed (**figure 3**). Given the widespread uncertainty accompanying the COVID-19 pandemic, readers should temper optimism for now. It is promising, however, that the number of responses to this year's survey increased 44 percent[7] over last year and exceeds all prior participation.

Enterprises that were permitted to remain open may have been susceptible to hiring freezes and other budgetary impacts to keep the lights on and minimize financial loss. Reports of work reductions and salary cuts in the cybersecurity industry show that it was not immune to business operational adjustments.

Although the cybersecurity industry continues to be a seller's market,[8] the global pandemic appears to have positively influenced cybersecurity staff retention efforts. As last year's survey revealed, staffing levels, retention and cyberattacks are somewhat interrelated. Not only do 68 percent of respondents whose organizations experienced more cyberattacks in the past year report being somewhat or significantly understaffed, but 63 percent of

[3] (ISC)²®, *Cybersecurity Professionals Stand Up to a Pandemic*, (ISC)² Cybersecurity Workforce Study, 2020, www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx
[4] Goldstein, M.; P.G. Martinez; S. Papineni; J. Wimpey; "The Global State of Business During COVID-19: Gender Inequalities," World Bank Blogs, 8 September 2020, https://blogs.worldbank.org/developmenttalk/global-state-small-business-during-covid-19-gender-inequalities
[5] McKinsey & Company, "COVID-19: Briefing note #49, April 7, 2021," COVID-19: Implications for business, 7 April 2021, www.mckinsey.com/business-functions/risk/our-insights/covid-19-implications-for-business
[6] (ISC)²® reports that 17 percent of respondents reported a reduction in hours, and 19 percent reported a reduction in salary. See *Op cit* (ISC)²®.
[7] The 2021 State of Cybersecurity survey received 3,659 responses, compared with 2,051 responses to the 2020 survey.
[8] The sellers are the cybersecurity job applicants (or employees), while the buyers are the hiring enterprises that are seeking qualified candidates.

the respondents whose organizations experienced more attacks indicate they have experienced difficulties retaining qualified cybersecurity professionals. Additionally, 65 percent of respondents whose cybersecurity teams are significantly understaffed say they have experienced difficulties retaining qualified cybersecurity professionals—conceivably due to burnout.[9, 10]

Although the cybersecurity industry continues to be a seller's market, the global pandemic appears to have positively influenced cybersecurity staff retention efforts.

Vacancies

Fifty-five percent of survey respondents claim to have unfilled cybersecurity positions (**figure 4**), which closely resembles last year's data (57 percent). The survey results indicate a significant improvement in the amount of time required to fill a cybersecurity position (**figure 5**), with a double-digit decrease in the percent of respondents whose organizations take more than six months to fill vacant positions.

FIGURE 3: Cybersecurity Staffing

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

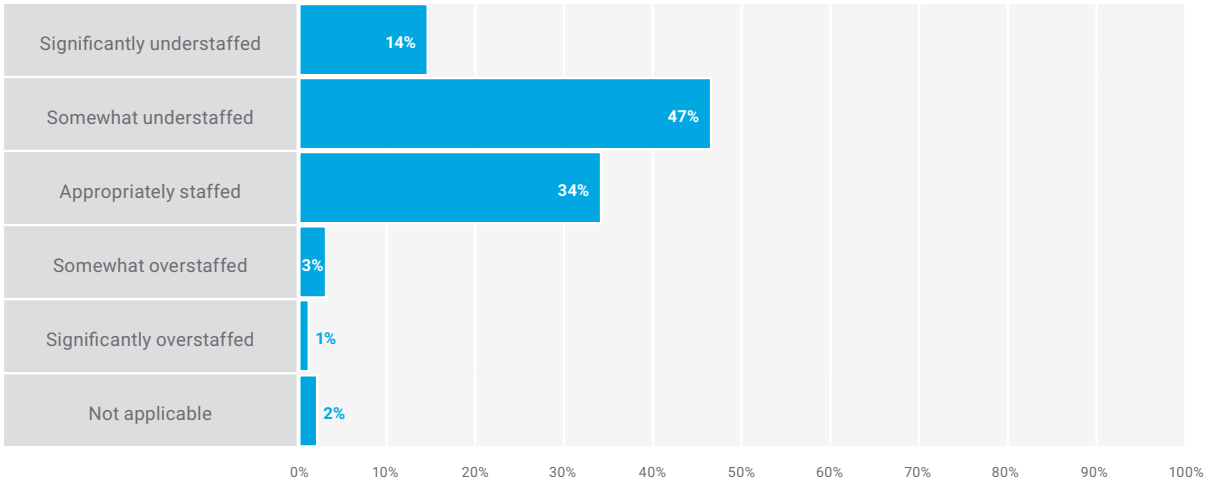
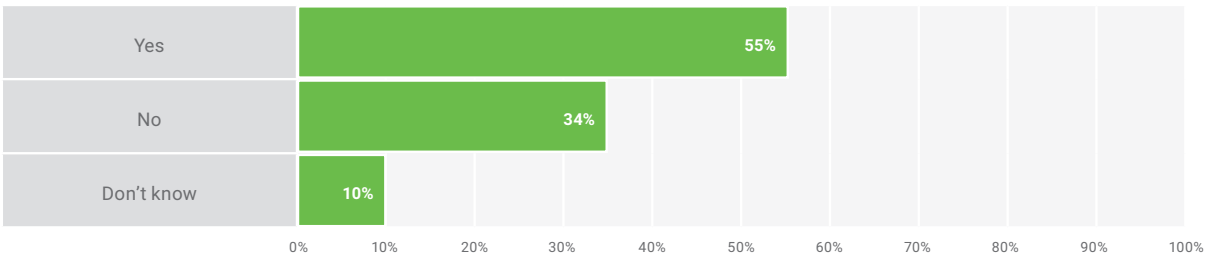


FIGURE 4: Unfilled Positions

Does your organization have unfilled (open) cybersecurity positions?



[9] Paterson, J.; "Pandemic Burnout: Yes, It's a Thing. And It's a Security Risk," Security Boulevard, 14 October 2020, https://securityboulevard.com/2020/10/pandemic-burnout-yes-its-a-thing-and-its-a-security-risk/

[10] Palmer, D.; "How remote working is making life easier for hackers," ZDNet, 12 January 2021, www.zdnet.com/article/cybersecurity-teams-are-struggling-with-burnout-but-the-attacks-keep-coming/

Technical cybersecurity positions were again the top vacancy reported this year (**figure 6**); however, the percent of respondent enterprises with positions left unfilled increased this year, between two and five percentage points, for every position.

Some positive news—however slight—is that managers and directors who are exploring new opportunities have more available to them. **Figure 7** shows year-over-year reporting data of unfilled positions.

When asked about future demand (**figure 8**), respondents expect no meaningful change from last year's survey results across the five categories of positions. **Figure 9** shows four-year trending on future demand, which appears to signal a leveling off.

Some positive news—however slight—is that managers and directors who are exploring new opportunities have more available to them.

However, post-pandemic data will be required to ascertain the ultimate effect of COVID-19 and workforce development initiatives on cybersecurity human capital.

FIGURE 5: Time to Fill a Cybersecurity Position

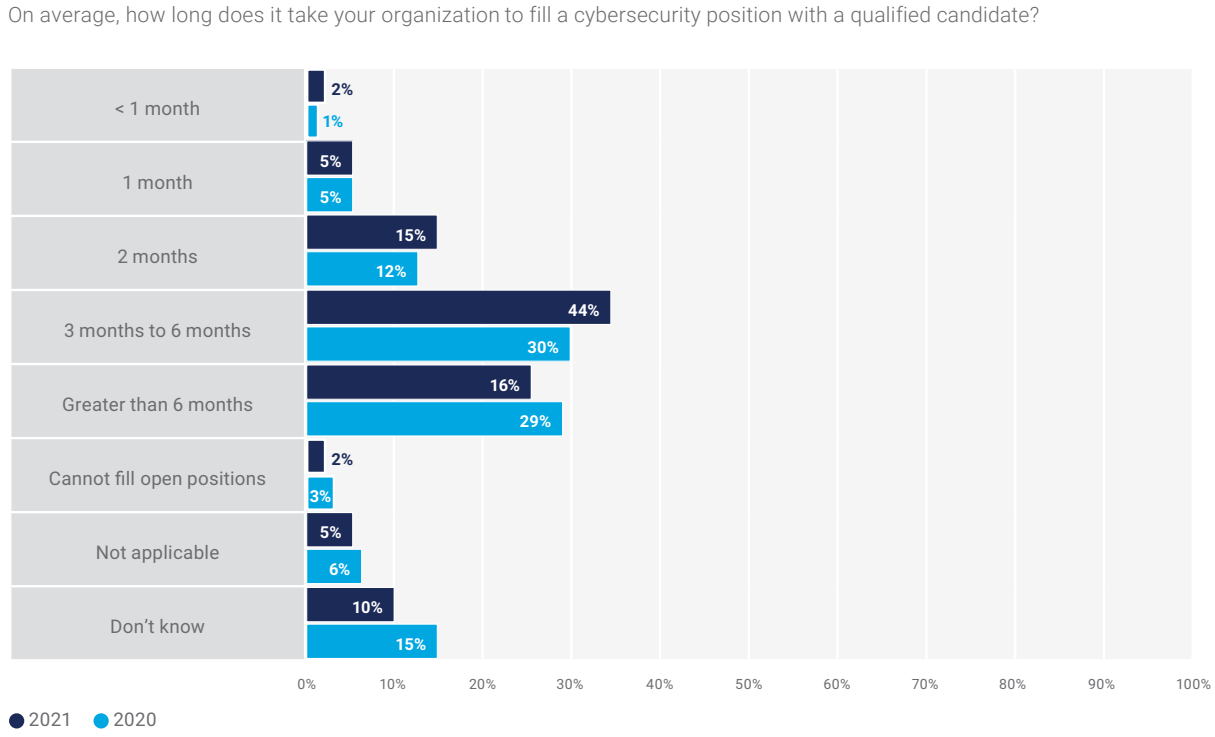


FIGURE 6: Percentages of Unfilled Positions at Given Organizational Levels

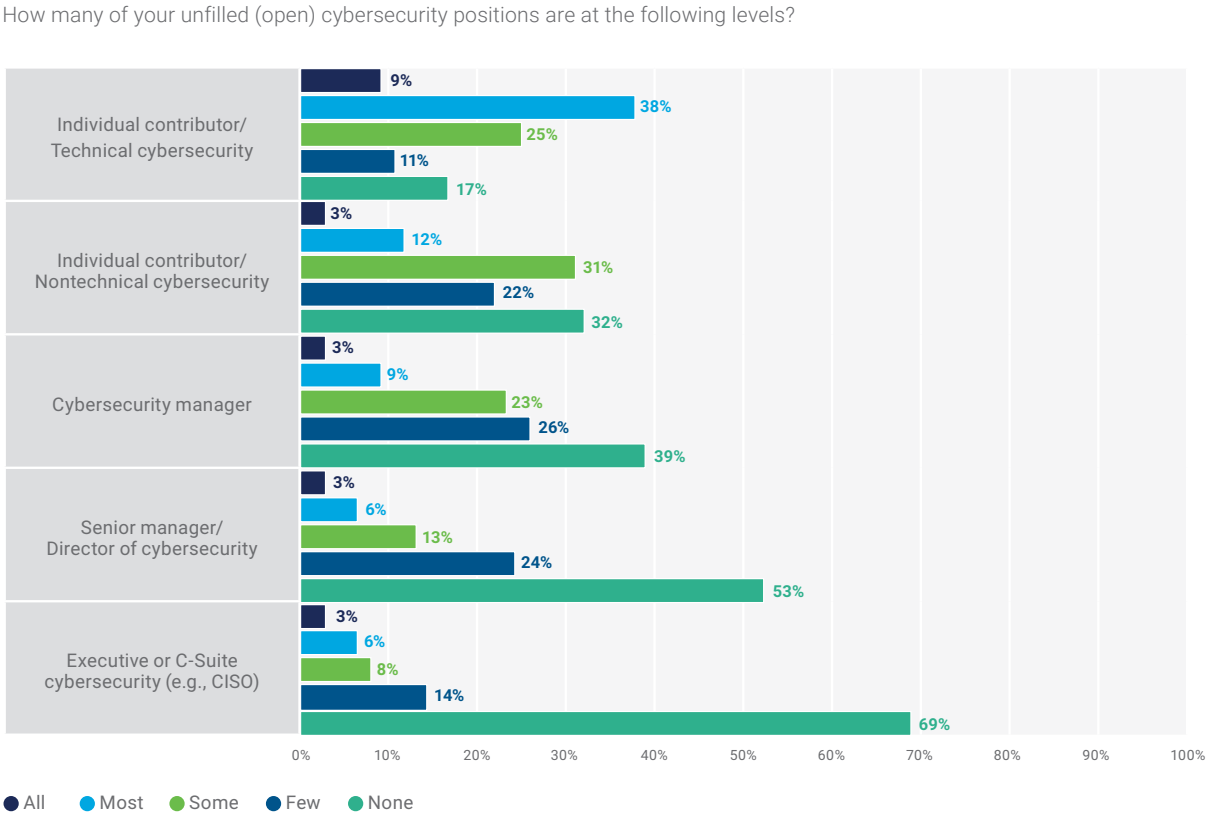
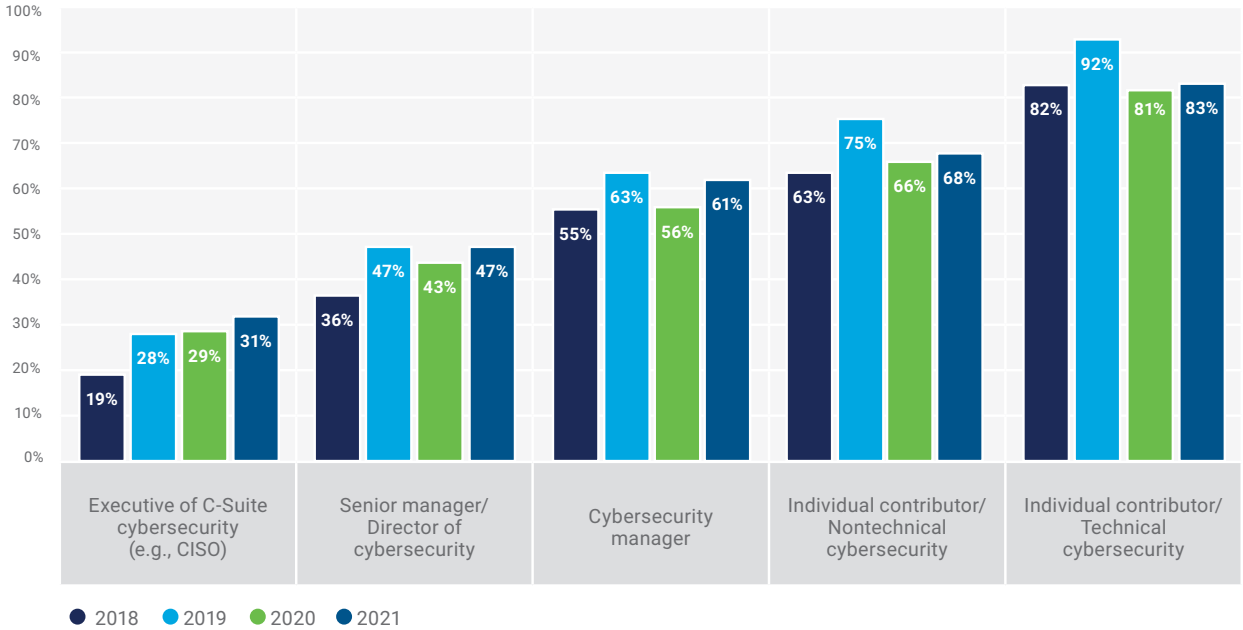


FIGURE 7: Unfilled Position Reporting for 2018-2021[11]



[11] This figure compares the unfilled position data from 2018-to-2021 ISACA State of Cybersecurity reports. Percentages represent the sum of all reported vacancy percentages for each position and exclude the "None" response percentages.

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?

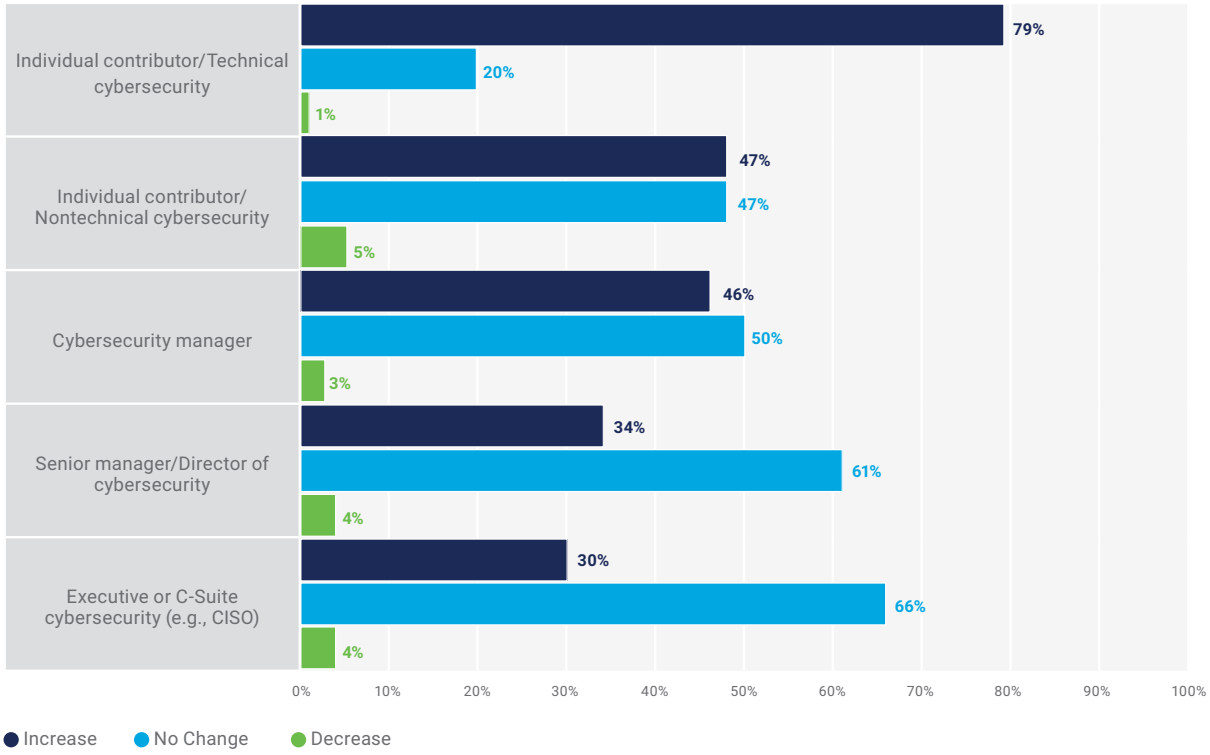
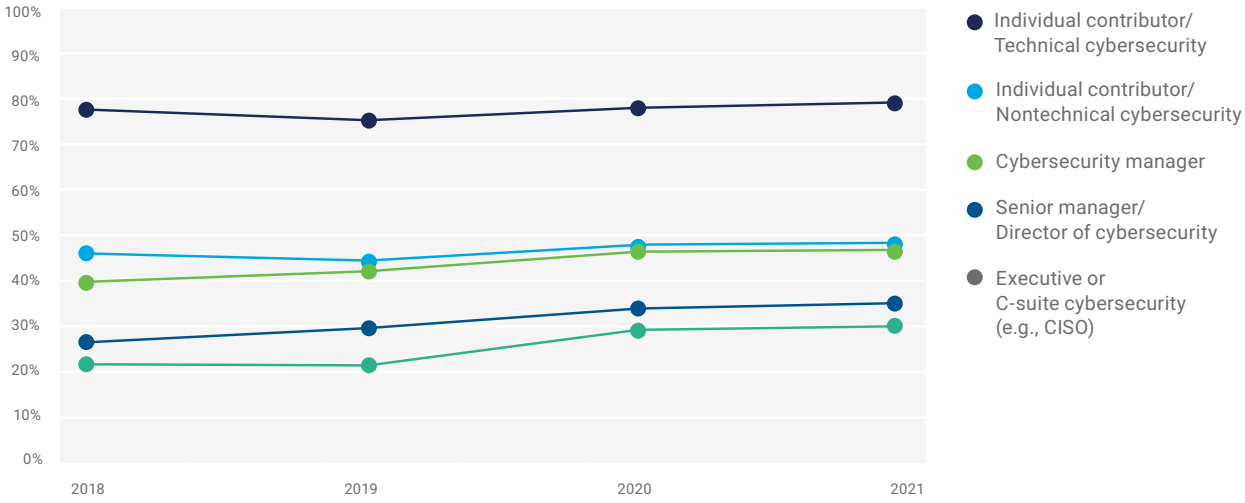


FIGURE 9: Hiring Demand Trending (2018-2021)



Pipeline Challenges

Survey data extend previous reporting that hiring managers have low confidence in cybersecurity applicants. **Figure 10** shows that 50 percent of those surveyed generally do not believe that their applicants are well qualified, and an additional 16 percent are either unable or uncomfortable making the determination. As was the case last year, this data point translates to delays in filling positions. Seventy-two percent of those who reported that fewer than 25 percent of their applicants are well qualified have unfilled positions longer than three months.

Hands-on cybersecurity experience remained the primary factor in determining whether a candidate is considered qualified (**figure 11**). As reported last year—and up by four percentage points—the largest skills gap among cybersecurity professionals is soft skills, e.g., communication, flexibility and leadership (**figure 12**)**.** The likelihood that increased remote work contributed to this change must be considered.

The second-largest skills gap—security controls implementation—came in a distant 20 percentage points behind soft skills. Other notable gaps include software development-related topics (e.g., languages, machine code, testing and deployment), data-related topics (e.g., characteristics, classification, collection, processing and structure), coding skills and networking-related topics (e.g., architecture, addressing and networking components).

FIGURE 10: Percentage of Cybersecurity Applicants Who Are Well Qualified

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

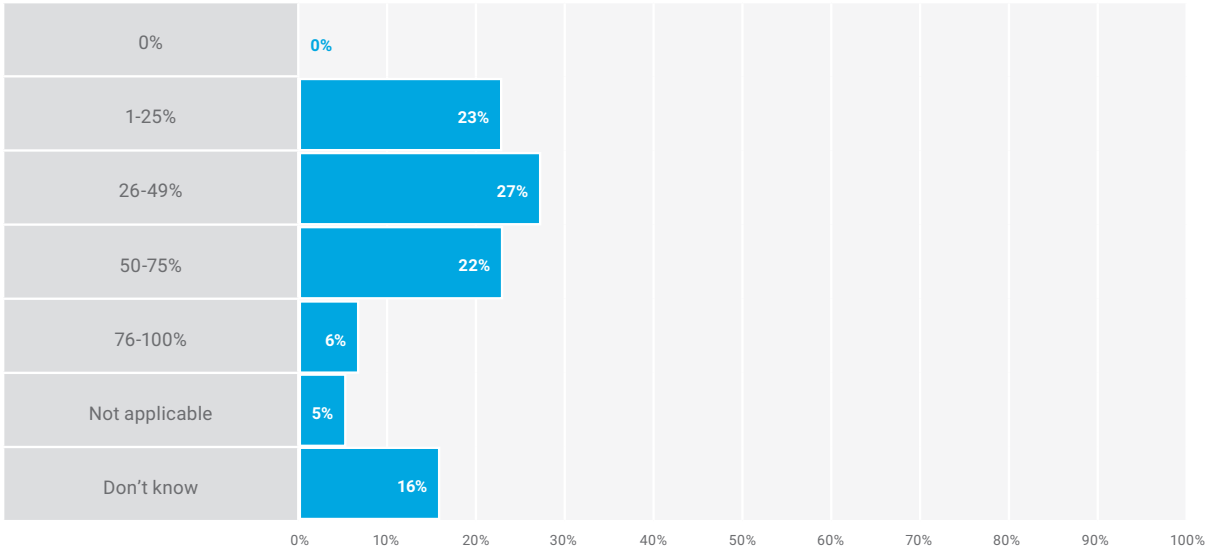


FIGURE 11: Candidate Qualifications

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

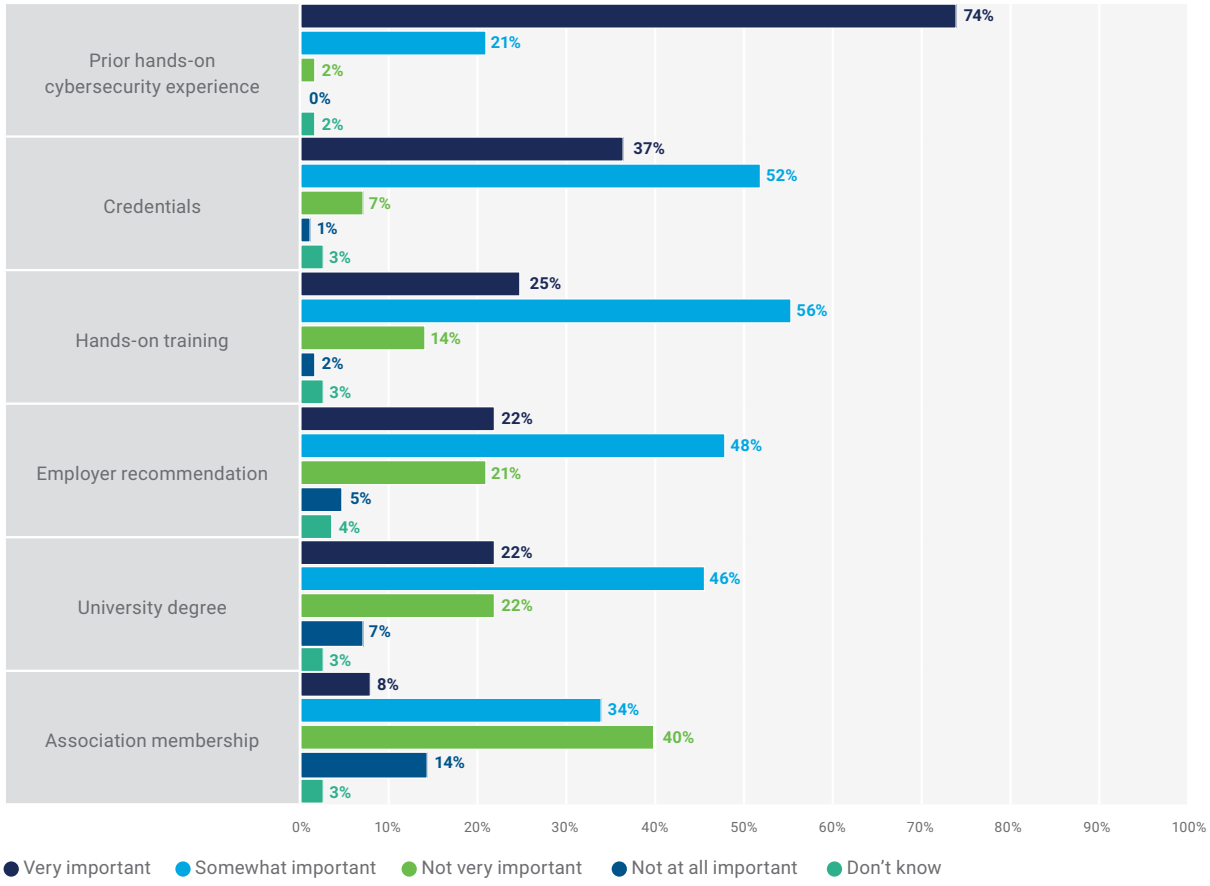
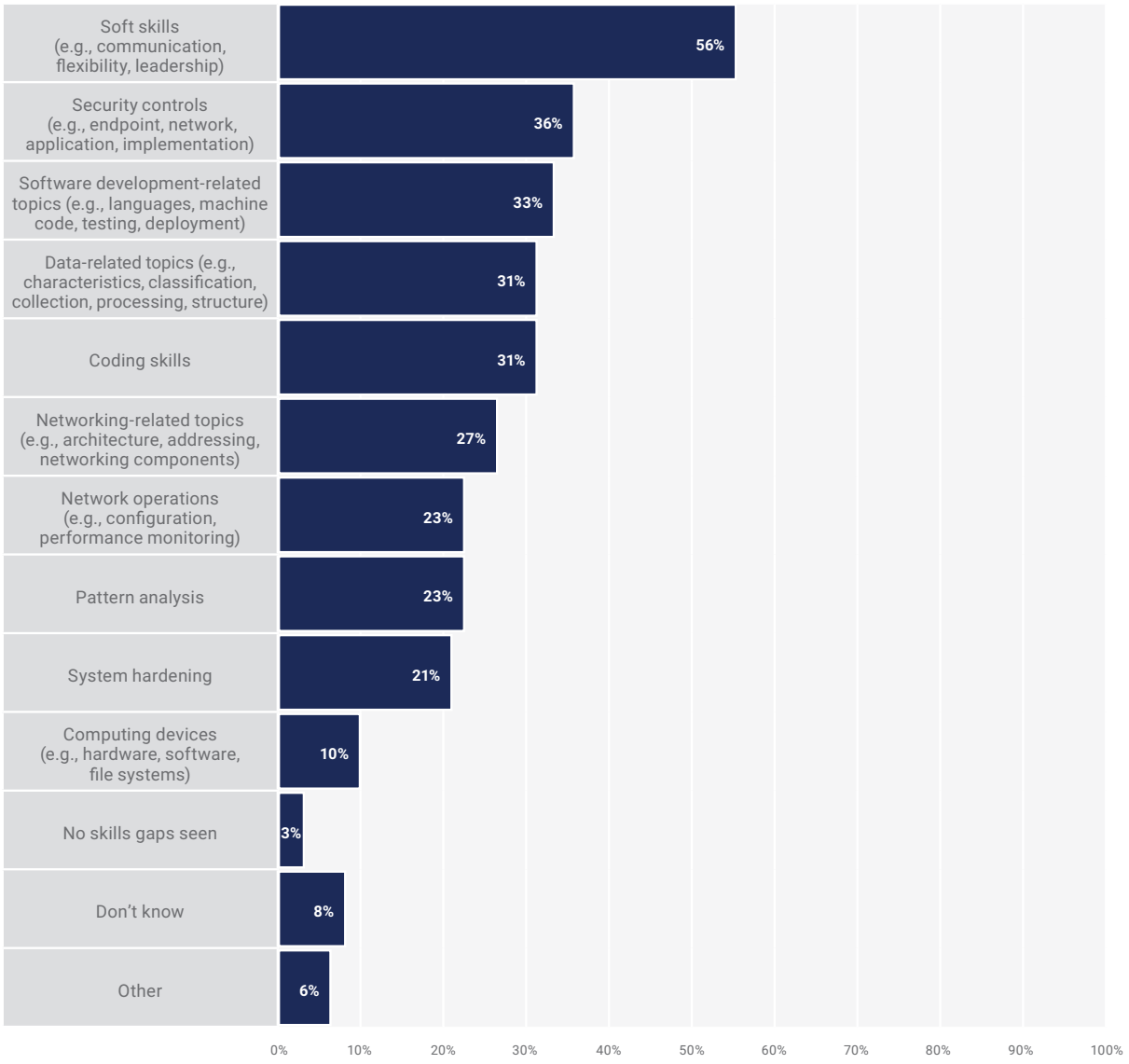


FIGURE 12: Quantified Skills Gap

What are the biggest skill gaps you see in today's cybersecurity professionals? Select all that apply.



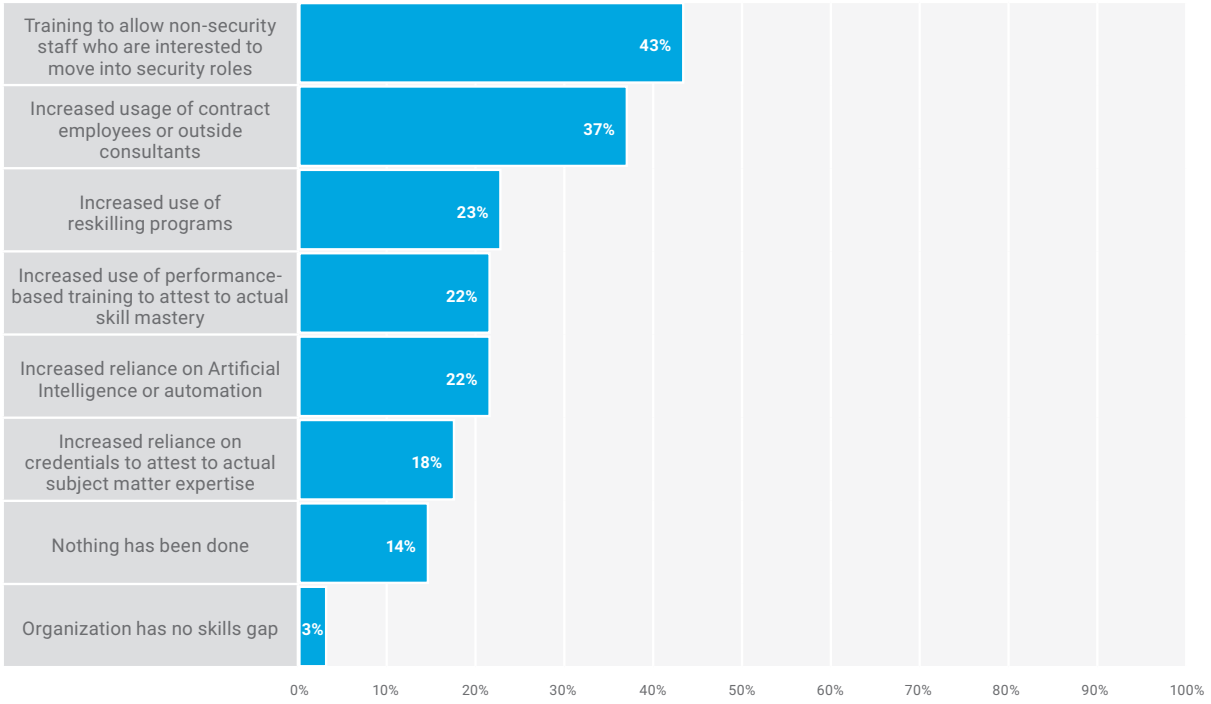
Employer Actions

The actions that enterprises are taking to address perceived skills gaps closely resemble those reported last year (figure 13). Cross-training of enterprise personnel and increased use of contractors and consultants remain primary mitigations.

Training increases three percentage points from last year, while contractors or consultants dips three percentage points. Artificial intelligence increases slightly to 22 percent (from 20 percent), and reliance on credentials slips two percentage points from a year ago.

FIGURE 13: Means of Mitigating Shortfalls

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



Education vs. Training

University education remains a common, albeit imperfect, means of supplying the talent pipeline. Respondents remain split about whether a university degree well prepares recent graduates for the cybersecurity challenges facing enterprises (**figure 14**). Despite this division, 58 percent of respondents report that their organizations require a degree (**figure 15**), although this requirement varies greatly by geographic area. **Figure 16** shows the regional percentage of enterprises that require a university degree for entry-level cybersecurity positions, based on 2020 and 2021 report data, and indicates how each is trending.

When asked about skills gaps among recent university graduates, respondents again highlight soft skills (**figure 17**). Given the vast number of organizations that require a university degree for entry-level positions, the lack of soft skills is concerning and needs to be addressed. The technical skills that survey respondents find most lacking in recent graduates (**figure 17**) suggest omissions or inadequacies within university programs regarding networking and hardening.

FIGURE 14: Cybersecurity Degree Confidence

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

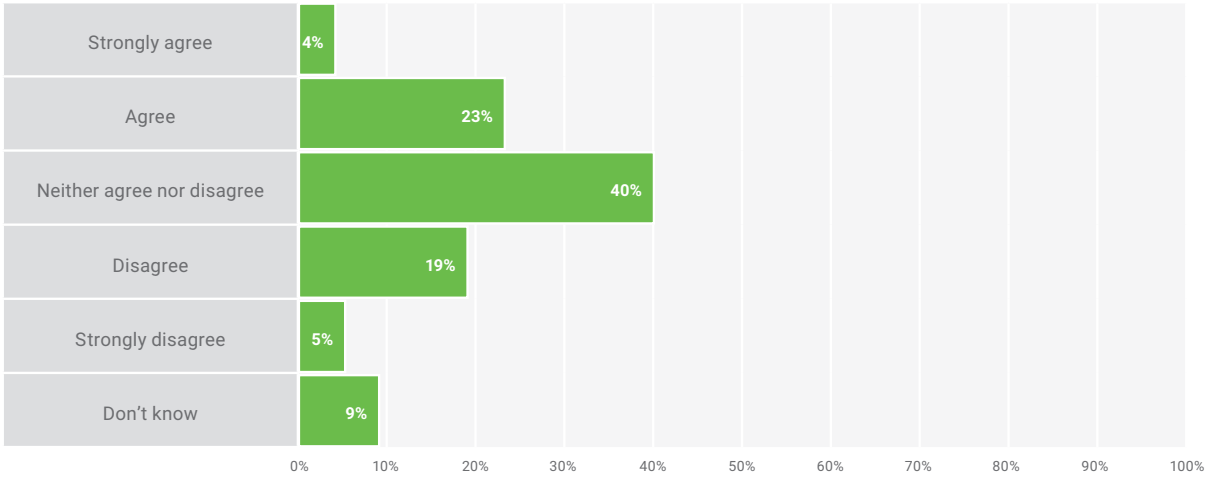


FIGURE 15: University Requirements

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

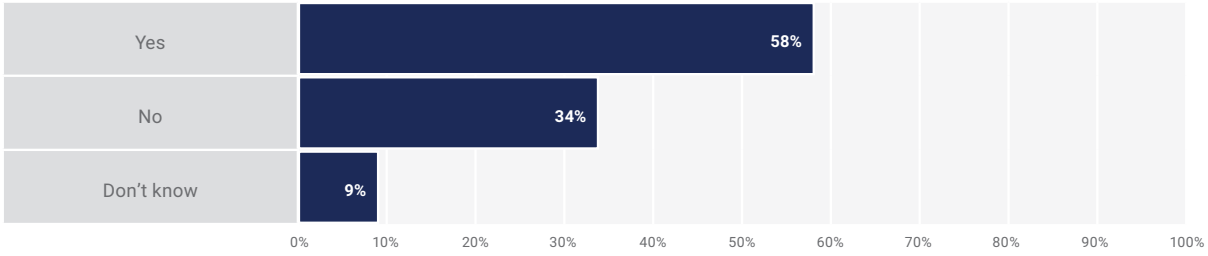


FIGURE 16: 2020-2021 Entry-Level Degree Requirement Percentages by Region

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

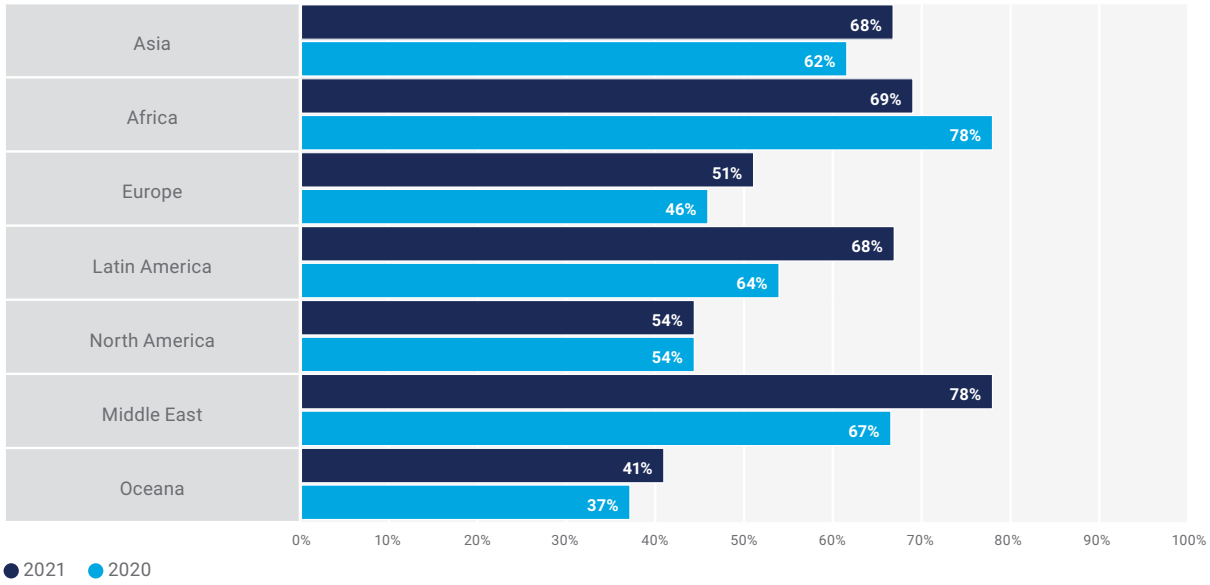
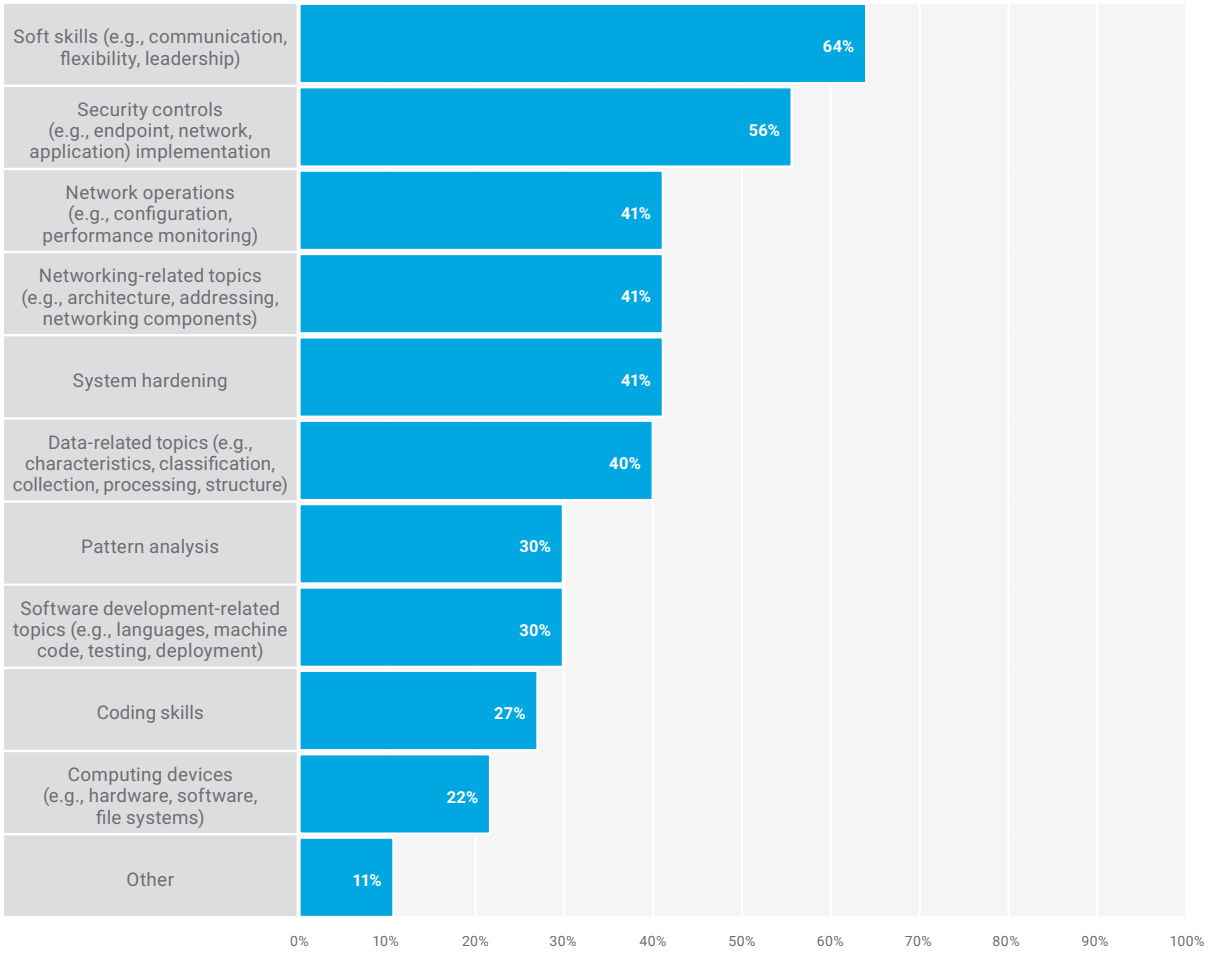


FIGURE 17: Skills Gap Among Recent Graduates

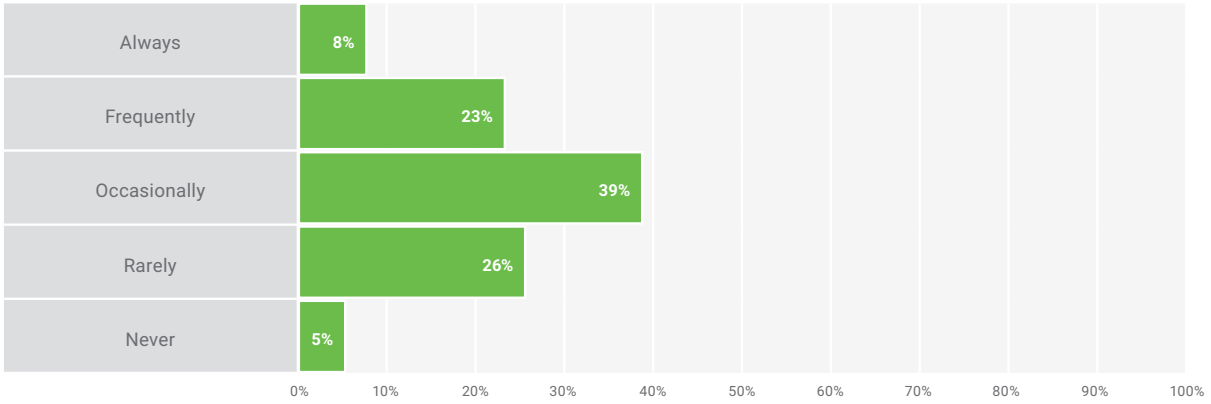
Which of the following skills gaps have you noticed among recent university graduates? Select all that apply.



Recruitment remains a challenge for many. Survey data shown in **figure 18** illustrate the disconnect between hiring managers and those charged with sourcing candidates—just 31 percent feel that their human resources (HR) department fully understands their hiring needs. Closing this gap remains aligned closely to shortening the time to fill open positions. Of those respondents who report that HR always or frequently understands their cybersecurity hiring needs, 30 percent hire in less than two months, which is consistent with last year's survey data.

FIGURE 18: HR Needs Comprehension

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



Retention Positivity

Although COVID-19 poses a wide range of challenges, survey data indicate it mitigated retention woes during 2020. Just 53 percent of survey respondents indicate difficulty retaining talent—a four percentage-point decline from the previous year.

Although COVID-19 poses a wide range of challenges, survey data indicate it mitigated retention woes during 2020.

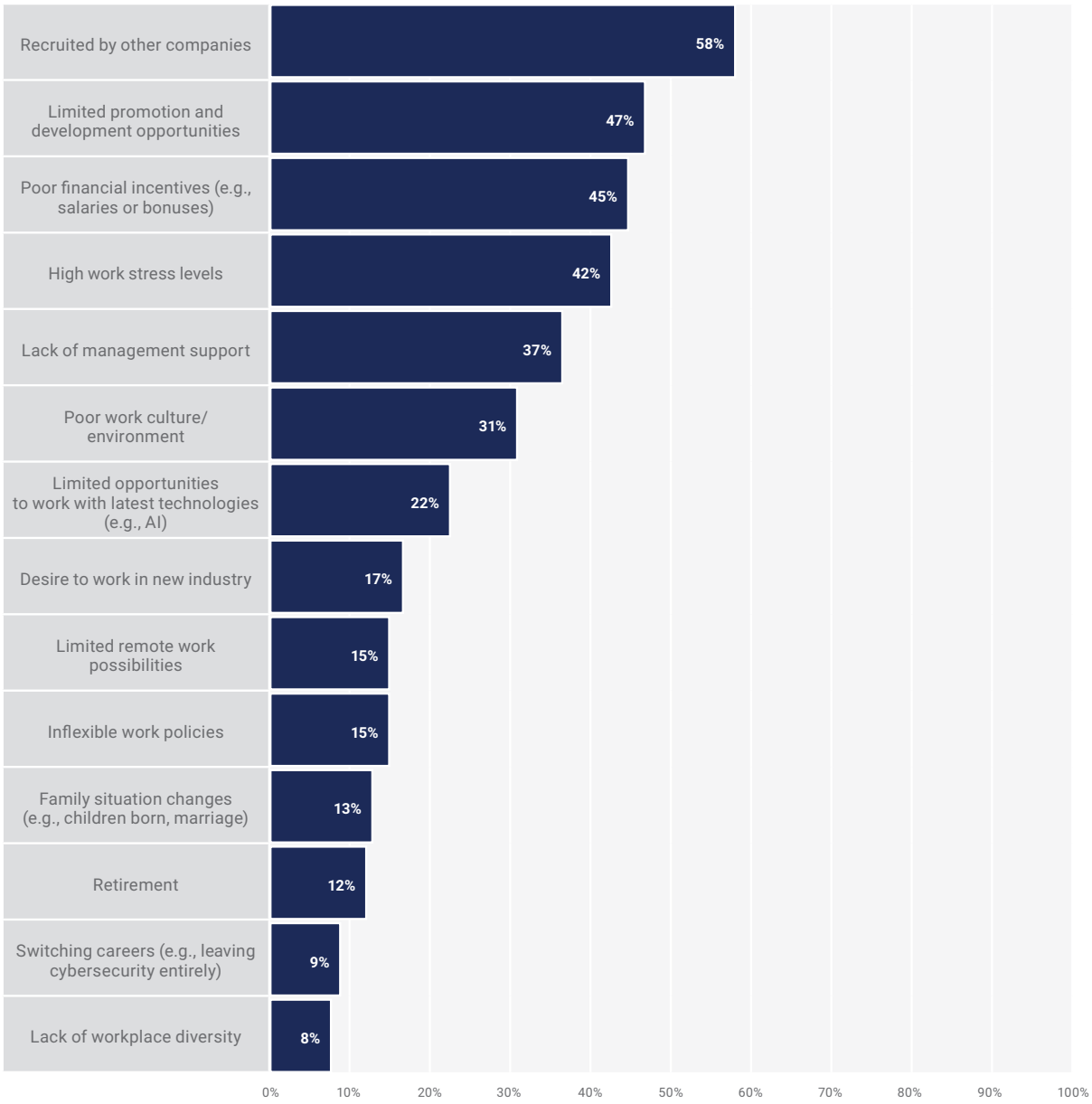
The factors that survey respondents attribute to causing cybersecurity professionals to leave their current positions (**figure 19**) largely resemble those from a year ago, with a few exceptions.

The poor financial incentives (e.g., salaries or bonuses) factor decreases from 50 percent a year ago to 45 percent this year, which suggests respondents are fully aware of the financial uncertainty facing employers. Remote work possibilities increased throughout the pandemic due to governmental mandates affecting employers.

The percentage of respondents who think that limited remote work possibilities are a factor for employees leaving cybersecurity positions decreases six percentage points from the previous year to 45 percent. Two factors increased three percent from the previous-year survey results—leaving the industry and retirement. Ultimately, time will reveal the pandemic's influence on these noted changes.

FIGURE 19: Why Cybersecurity Professionals Leave Their Jobs

Which, if any, of the following reasons do you feel are causing cybersecurity professionals to leave their current jobs? Select all that apply.

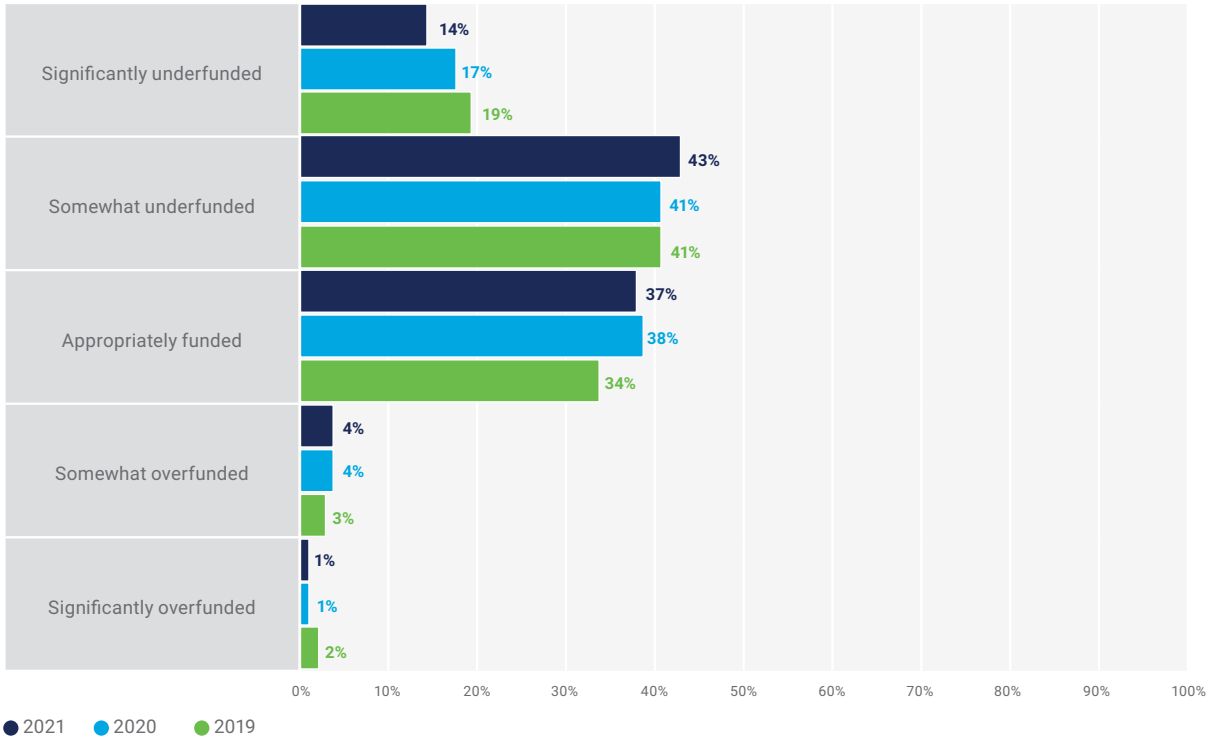


Has Cybersecurity Funding Reached an Apex?

According to last year's survey results,[12] cybersecurity budget forecasts were projected to bounce back; however, when asked about current funding levels, respondents indicate no improvement to cybersecurity budgetary funding. However, this does not mean that there has been no net gain year over year, because data show a steady decrease in the significant underfunded category (**figure 20**)**.** Survey respondents appear discouraged about the next-year budget outlook, with 20 percent expecting a decline in funding (**figure 21**). In recognition of COVID-19's potential influence on responses, this year's survey includes an additional question about pandemic spending (**figure 22**). One-third of respondents indicate that their organizations spent unplanned money on new security initiatives. However, multiyear data (**figure 23**) reveals optimism for budget increases is at a three-year low, second only to 2017 data. Last year, ISACA reported the possibility of budget leveling, which carries forward with this year's data and is reinforced by an absence of any significant reactive COVID-19 security spending (**figure 22**)**.**

FIGURE 20: Cybersecurity Funding Perception

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



[12] ISACA, *State of Cybersecurity 2020, Part 1: Global Update on Workforce Efforts and Resources*, 2020, www.isaca.org/bookstore/bookstore-wht_papers-digital/whpsc201

FIGURE 21: Enterprise Security Budget Outlook

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

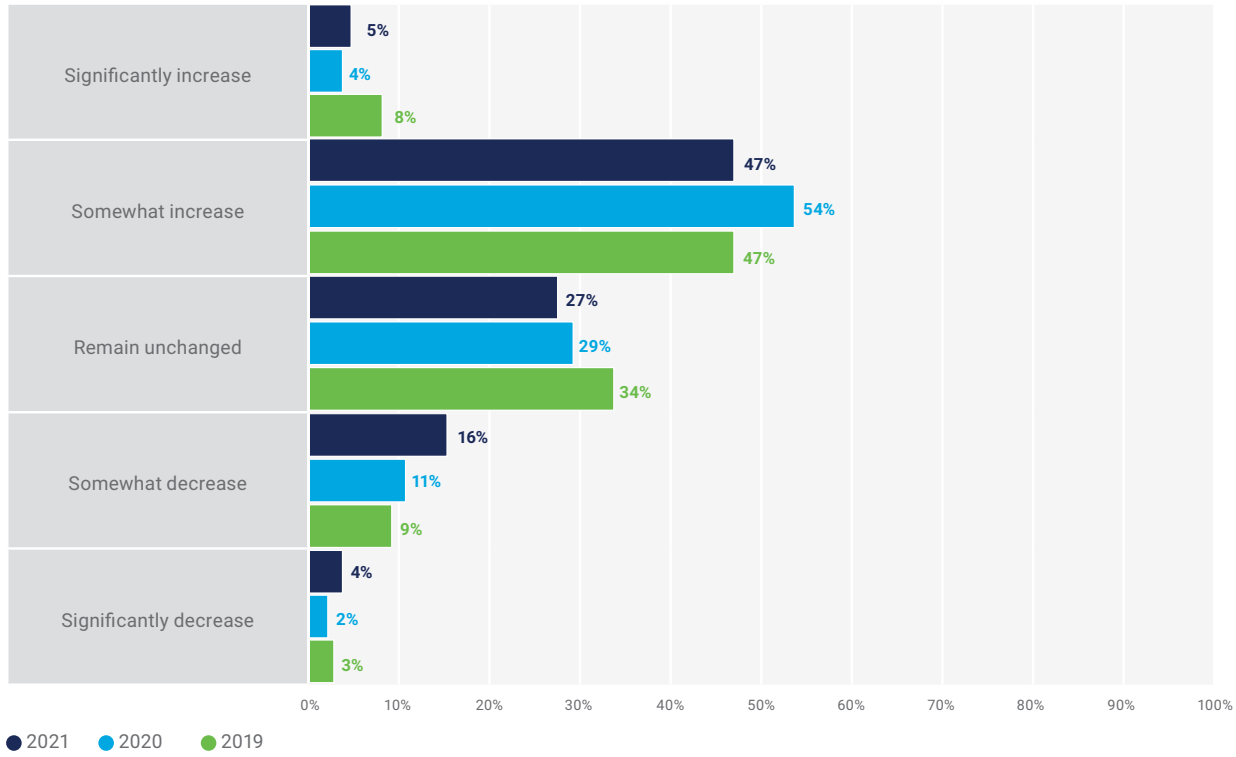


FIGURE 22: Pandemic Specific Technology Spending

Has your organization increased its spending specifically on new security technology initiatives during the COVID-19 pandemic?

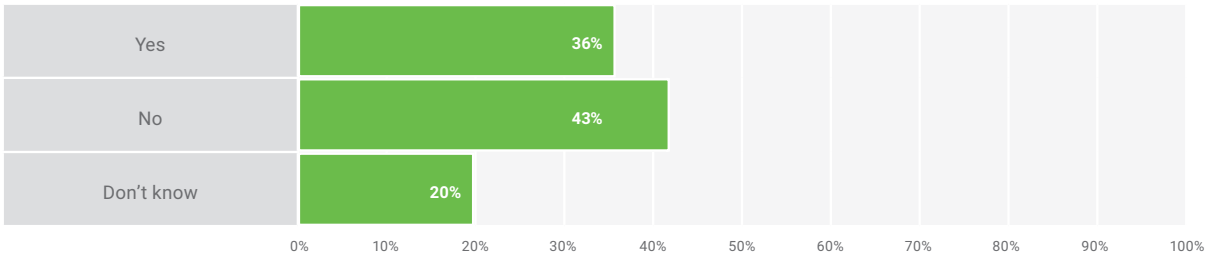
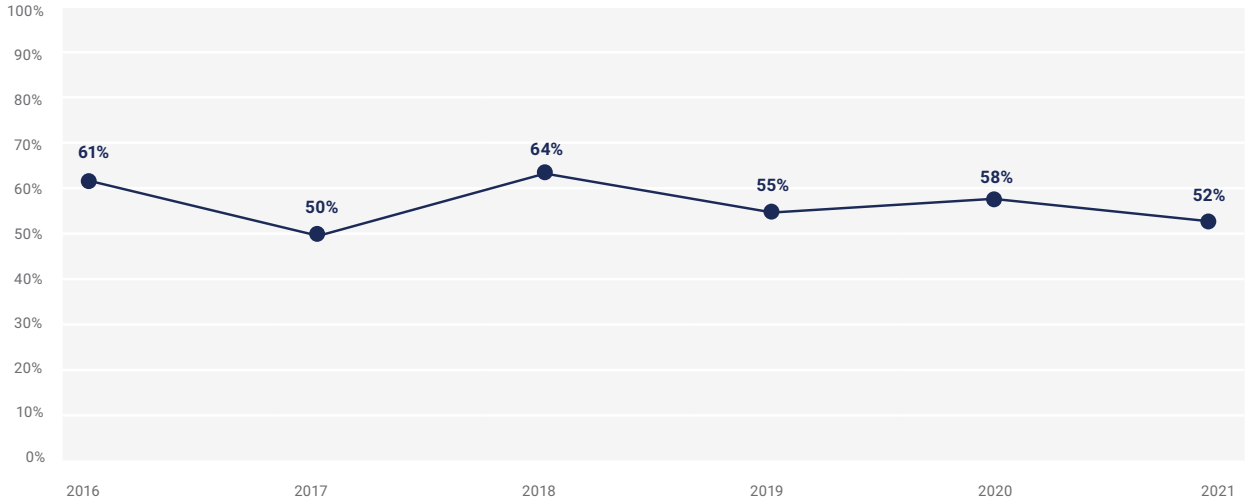


FIGURE 23: Forecasted Security Budget Increases (5 Year)



What Now?

For many years, ISACA and others have been reporting on the imbalance between supply and demand for cybersecurity talent. ISACA annual surveys show no evidence that the efforts of governments, academia and industry have made any real headway to correct this imbalance.[13] Why has so little headway been made when, for years, the shortage of cybersecurity talent has been acknowledged as a large problem? Why is society not tackling this problem with more direction and funding, given its importance in sustaining life as we know it in the twenty-first century? This section addresses these questions.

Each year, respondents confirm that prior cybersecurity experience carries more weight than university degree programs (**figure 11**), yet the requirement that qualified candidates have a university degree continues to rank highly. Ultimately, university programs and other workforce development initiatives offer little upside without substantial increases in the number of entry-level positions or, at the very least, rightsizing position descriptions that enterprises believe are necessary to source the best candidates.

It is increasingly obvious that the industry requires recalibration. ISACA solicited input from US and European governmental bodies, industry participants, and an apprenticeship program to add depth to this report.

It is increasingly obvious that the industry requires recalibration.

Rodney Petersen, Director, National Initiative for Cybersecurity Education, National Institute of Standards and Technology, US Department of Commerce, used a US baseball analogy to encourage employers to "commit to the development of a farm team[14] of prospects"[15] for future cybersecurity leaders. There is no quick solution to the shortage and the entire continuum must be considered—from early learning through on-the-job skills maintenance.

[13] ISACA Global remains concerned that the situation continues to be the same year-over-year. As a nonprofit association, ISACA works with industry, government and apprenticeship programs, but the needle has not moved. Those passionate about this issue are encouraged to join the ISACA Engage Community: Information and Cybersecurity to continue the discussion.
[14] In US baseball, a farm team is analogous to a river tributary. It is a less robust team whose role in the program is to provide experience and training that allows successful new players to move to a higher-level team.
[15] Petersen, R.; interview conducted by ISACA

National Initiative for Cybersecurity Education

The National Initiative for Cybersecurity Education (NICE) program office serves the US government, academia and industry, along with individuals and organizations focused on growing and sustaining the US cybersecurity workforce.

NICE recently updated is strategic plan[16] and its Workforce Framework for Cybersecurity.[17] NICE Framework draft competencies are under review. NICE continues to engage US K-12 educators, industry and the federal workforce through a myriad of initiatives.

According to Peterson, "there is too much emphasis on mid- and senior-level positions or capabilities without enough entry-level opportunities for new workers or those who seek to reskill."[18] With a renewed strategy, NICE recently restructured its collaborative framework. In November 2020, NICE transitioned the former NICE Working Group to the NICE Community Coordinating Council[19] and subsequently retired subworking groups, which typically comprised government, certification bodies, academia and training providers.

The restructuring resulted in three NICE working groups and four communities of interest. Working groups include Modernize Talent Management,[20] Promote Career Discovery[21] and Transform Learning Process[22]. Communities of interest include Apprenticeships in Cybersecurity,[23] Cybersecurity Skills Competitions,[24] K12 Cybersecurity Education[25] and NICE Framework Users.[26]

European Union Agency for Cybersecurity

The European Union Agency for Cybersecurity (ENISA) serves European Union (EU) citizens, students and organizations across member states, and contributes to cybersecurity policy, preparedness and resilience. ENISA authored *Cybersecurity Skills Development In The EU*[27] and the *Cybersecurity Higher Education Database* (CyberHEAD), and is currently working on a skills framework.

ENISA has acknowledged that "Europe lags behind in the development of a comprehensive approach to define a set of roles and skills relevant to the cybersecurity field."

According to Fabio Di Franco, seconded national expert, ENISA, CyberHEAD[28] is the largest validated cybersecurity higher education database in the EU and European Free Trade Association (EFTA) countries, and the primary reference for those looking to upskill.[29]

ENISA has acknowledged that "Europe lags behind in the development of a comprehensive approach to define a set of roles and skills relevant to the cybersecurity field."[30] The EU has prioritized development of the European Cybersecurity Skills Framework to address the growing

[16] NIST, *National Initiative for Cybersecurity Education (NICE), Strategic Plan*, 18 March 2021, www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan
[17] NIST, NICE Framework Resource Center, www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center
[18] *Op cit* Petersen
[19] NIST, NICE Community Coordinating Council, www.nist.gov/itl/applied-cybersecurity/nice/about/community-coordinating-council
[20] National Institute of Standards and Technology (NIST), National Initiative for Cybersecurity Education (NICE), "Modernize Talent Management Working Group," www.nist.gov/itl/applied-cybersecurity/nice/about/community-coordinating-council/modernize-talent-management
[21] National Institute of Standards and Technology (NIST), National Initiative for Cybersecurity Education (NICE), "Promote Career Discovery Working Group," www.nist.gov/itl/applied-cybersecurity/nice/about/community-coordinating-council/promote-career-discovery
[22] National Institute of Standards and Technology (NIST), National Initiative for Cybersecurity Education (NICE), "Transform Learning Process Working Group," www.nist.gov/itl/applied-cybersecurity/nice/about/community-coordinating-council/transform-learning-process
[23] National Institute of Standards and Technology (NIST), National Initiative for Cybersecurity Education (NICE), "Apprenticeships in Cybersecurity Community of Interest," www.nist.gov/itl/applied-cybersecurity/nice/about/community-coordinating-council/apprenticeships-cybersecurity
[24] National Institute of Standards and Technology (NIST), National Initiative for Cybersecurity Education (NICE), "Cybersecurity Skills Competitions Community of Interest," www.nist.gov/itl/applied-cybersecurity/nice/about/community-coordinating-council/cybersecurity-skills
[25] National Institute of Standards and Technology (NIST), National Initiative for Cybersecurity Education (NICE), "K12 Cybersecurity Education Community of Interest," www.nist.gov/itl/applied-cybersecurity/nice/about/community-coordinating-council/k12-cybersecurity-education
[26] National Institute of Standards and Technology (NIST), National Initiative for Cybersecurity Education (NICE), "NICE Framework Users Group," www.nist.gov/itl/applied-cybersecurity/nice/about/community-coordinating-council/nice-framework-users
[27] European Union Agency for Cybersecurity (ENISA), *Cybersecurity Skills Development in the EU*, December 2019, www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union/at_download/fullReport
[28] European Union Agency for Cybersecurity (ENISA), "Cyberhead," www.enisa.europa.eu/topics/cybersecurity-education/cyberhead/view
[29] DiFranco, F.; interview conducted by ISACA
[30] European Union Agency for Cybersecurity (ENISA), "European Cybersecurity Skills Framework," www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework

economic and national security issues caused by the cybersecurity skills shortage plaguing member states.

An *ad hoc* working group (AHWG) serves to harmonize cybersecurity education, training and workforce development ecosystems with the following planned deliverables:

- Unambiguous taxonomy of skills, competences and occupations in the cybersecurity workforce
- List of cybersecurity profiles and associated skills, competences, responsibilities, accountabilities and tasks
- Analysis of a detailed cybersecurity workforce market in Europe
- Common cybersecurity skills and competencies for Europe

According to Di Franco, this requires the AHWG to:

- Create a specialized job roles and skills framework for cybersecurity professionals
- Create an inventory of current labor in cybersecurity
- Advise on how to enforce the European cybersecurity workforce capacity building
- Formulate proposals on how to identify and reduce the potential cybersecurity skills shortage with sufficient specificity of competencies and roles

ISACA is eager to see how the European Cybersecurity Skills Framework compares with the NICE Workforce Framework for Cybersecurity.

Workforce Development Perspective

Apprenticeships continue to gain momentum in the United States without commonality and despite an inability to scale.[31]

CyberUp is a US-based talent pipeline supplier that serves adults and youth to teach them cybersecurity skills, with the intention of connecting them to employment opportunities.[32] Initiatives include 16-week part-time pre-apprenticeship training, which helps individuals acquire entry-level certification and placement with an employer for one year, as an apprentice. CyberUp fully embraces the need to engage students early in life. One way it does this is through monthly cybersecurity competitions for students, typically aged 11 to 18.

According to CyberUp Executive Director Tony Bryan, the largest barrier is the mindset that industry faces a skills gap as opposed to a talent pipeline problem. Employers still use 20-year-old hiring practices (internship and co-op) and must reimagine hiring. Pathways such as apprenticeship offer a low-cost, low-risk, faster way to ready a workforce.[33]

Plenty of programs exist to provide job skills, but employers are not equipped and ready to hire individuals from the different skill paths (traditional or nontraditional).

Industry Perspective

Enterprises continue to tackle this problem, often through partnerships, coalitions or outreach programs. For example, HCL Technologies partners with post-secondary/engineering degree education institutions and industry-leading vendors on technical orientation and enablement. HCL Technologies, among others, has established training or retraining programs to increase talent pools. Cybersecurity competitions are a popular means of attracting applicants who are not currently in formal cybersecurity roles.

Renju Varghese, Fellow & Chief Architect, CyberSecurity & GRC Services, HCL Technologies, echoes respondent sentiment of shortcomings in university programs. When asked about the largest barriers to decreasing the gap between cybersecurity supply and demand, Varghese highlighted a lack of technology skills among applicants and a shortage of those able to design secure systems, write safe computer code and detect malicious acts.[34]

[31] Most large-scale apprenticeship programs in the United States (e.g., construction, electricians, plumbers) are fostered by labor unions. To date, cybersecurity does not have a union nor widespread adoption in the United States.
[32] CyberUp, "Cultivating the Cybersecurity Talent Pipeline," https://wecyberup.org/
[33] Bryan, R.; interview conducted by ISACA
[34] Varghese, R.; interview conducted by ISACA

Conclusion: Business as Usual Is Not Working

The cybersecurity workforce shortage persists and likely will continue, until there is an honest analysis of what is and is not working. Despite years of effort by government, industry and academia, and despite the expenditure of large swaths of taxpayer dollars, little has changed.

Formal educational programs and industry cybersecurity training programs will never replicate cybersecurity experience, and employers must be willing to embrace their role in developing the cybersecurity leaders of tomorrow—a proposition that always carries risk that the employee may leave. However, employers alone cannot shoulder this responsibility—especially when the resounding skills gap is not technical, but rather soft skills. Notable examples of soft skills include communication skills, leadership, critical thinking, teamwork, work ethic and positive attitude. Of these, communication skills—verbal and written—can be taught but often require practice. Informal analysis of programs reveals that universities focus little here. Of specific interest to cybersecurity professionals is critical thinking, which includes analysis, interpretation, inference, explanation, self-regulation, open-mindedness and problem solving—all imperative skills for cybersecurity professionals. Although these skills can be taught, they are often more process-oriented and, therefore, are honed over time.

Although retention and fill data show improvement, these survey results require further trending to see whether betterments were due to the pandemic or to changing market conditions (e.g., employer expectations and compensation). Employers are wise to acknowledge and mitigate causal factors—after all, it is generally more cost-effective to retain employees than to hire and train new employees.

ISACA hopes that 2021 is the year that sizable decreases in time-to-hire and understaffing are realized. High-profile cybersecurity incidents[35] appear to have captured the attention of government and industry alike and may finally provide the necessary boost to make meaningful changes. However, cybersecurity career awareness and preparation efforts may be insufficient in areas across the globe that lack broadband connectivity.[36] In the meantime, the effect of technology on classrooms for students aged 11 to 18 can not be overlooked when the soft skills continue to be the major skills missing in the modern workplace.

[35] For example, SolarWinds and Microsoft Exchange Server
[36] In the United States, the FCC minimum standard for broadband is 25 Mbps down/3Mbps.

Acknowledgments

ISACA would like to recognize:

Board of Directors

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

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

Gabriela Hernandez-Cardoso
Independent Board Member, Mexico

Pam Nigro
CISA, CRISC, CGEIT, CRMA
Vice President–Information Technology, Security Officer, Home Access Health, USA

Maureen O'Connell
Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., USA

David Samuelson
Chief Executive Officer, ISACA, USA

Gerrard Schmid
President and Chief Executive Officer, Diebold Nixdorf, USA

Gregory Touhill
CISM, CISSP
President, AppGate Federal Group, USA

Asaf Weisberg
CISA, CRISC, CISM, CGEIT
Chief Executive Officer, introSight Ltd., Israel

Anna Yip
Chief Executive Officer, SmarTone Telecommunications Limited, Hong Kong

Brennan P. Baybeck
CISA, CRISC, CISM, CISSP
ISACA Board Chair, 2019-2020
Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

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

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

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 that effectively drive IT audit, risk management and security priorities forward. ISACA is a global professional association and learning organization that leverages the expertise of more than 150,000 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. In 2020, ISACA launched One In Tech, a philanthropic foundation that supports IT education and career pathways for under-resourced, under-represented populations.

About HCL

HCL Technologies (HCL) empowers global enterprises with technology for the next decade, today. HCL's Mode 1-2-3 strategy, based on its deep-domain industry expertise, client-centricity and entrepreneurial culture of Ideapreneurship™, enables businesses to transform into next-gen enterprises. HCL offers its services and products through three business units: IT and Business Services (ITBS), Engineering and R&D Services (ERS) and Products & Platforms (P&P). ITBS enables global enterprises to transform their businesses through offerings in the areas of applications, infrastructure, digital process operations and next generation digital transformation solutions. ERS offers engineering services and solutions in all aspects of product development and platform engineering. P&P provides modernized software products to global clients for their technology and industry specific requirements. Through its cutting-edge co-innovation labs, global delivery capabilities and broad global network, HCL delivers holistic services in various industry verticals, categorized as Financial Services, Manufacturing, Technology and Services, Telecom and Media, Retail and CPG, Life Sciences and Healthcare, and Public Services. As a leading global technology company, HCL takes pride in its diversity, social responsibility, sustainability, and education initiatives. For the 12 months ended Dec. 31, 2020 HCL had consolidated revenue of US$ 10.02 billion. Its 159,682 Ideapreneurs operate out of 50 countries. For more information, visit www.hcltech.com.

DISCLAIMER

ISACA has designed and created *State of Cybersecurity 2021, Part 1: Global Update on Workforce Efforts, Resources and Budgets* (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

Website: www.isaca.org

Provide Feedback:

www.isaca.org/state-of-cybersecurity-2021

Participate in the ISACA Online Forums:
https://engage.isaca.org/onlineforums

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAGlobal

Instagram:
www.instagram.com/isacanews/

CyberSecurity & GRC Services
by HCL Technologies

HCL

Inspiring business confidence through **dynamic cybersecurity**

Leader

Rated as a Leader by six leading industry analyst reports in FY'21 (Everest, ISG, Avasant)

6 CSFCs +
40 GDCs

450+
Global Customers

4500+
Experienced & Certified Engineers

for more info: **Cybersecurity-GRC@hcl.com**

www.hcltech.com