ISACA LOOKINGGLASS

State of Cybersecurity 2022

Global Update on Workforce Efforts, Resources and Cyberoperations

Security

CONTENTS

4 **Executive Summary**

4 **Survey Methodology**

7 **Lingering Global Pandemic Affects Staffing**
10 / Vacancies
14 / Pipeline Challenges
16 / University Insights
19 / Retention Challenges
20 / Employer Benefits
21 / Qualifying Workforce Issues
24 / Early Career Staff Insights
25 / Human Capital Mitigations

26 **Cybersecurity Budgets Near Equilibrium**

29 **Threat Landscape**
30 / An Abundance of Confidence
32 / Threat Actors and Attacks

35 **Cybersecurity Maturity—Barriers Limit Cyberrisk Assessment**

38 **Conclusion—Big News Is Not Always Big Data**

39 **Acknowledgments**

ABSTRACT

State of Cybersecurity 2022, Global Update on Workforce Efforts, Resources and Cyberoperations reports the results of the annual ISACA® global *State of Cybersecurity Survey*, conducted in the fourth quarter of 2021. This survey report focuses on the current trends in cybersecurity workforce development, staffing, cybersecurity budgets, threat landscape and cybermaturity. The survey findings reinforce past reporting and, in certain instances, mirror prior year data. Staffing levels, ease of hiring and retention remain pain points across the globe, and declining optimism about cybersecurity budgets reversed course this year.

Executive Summary

The eighth annual ISACA® global *State of Cybersecurity Survey* continues to identify current challenges and trends in the cybersecurity field. *State of Cybersecurity 2022* analyzes the survey results regarding cybersecurity staffing and skills, resources, cyberthreats and cybersecurity maturity. The survey findings are largely consistent with the findings from prior years indicating that enterprises continue to lack desired staffing levels and skills to combat cyberthreats:

- Any positive effect that the global COVID-19 pandemic had on retention last year wore off. Enterprises are engaged in a powerful battle to retain cybersecurity staff.
- Sixty-three percent of respondent enterprises have unfilled cybersecurity positions.
- Sixty percent of enterprises report experiencing difficulties in retaining qualified cybersecurity professionals.
- Soft skills and cloud-computing skills are the top two skill gaps that survey respondents see in today's cybersecurity professionals. Regarding recent university graduates, respondents highlight soft skills again this year as the area of greatest concern; however, technical skills appear to be improving.
- To address skill gaps, cross training of employees and increased use of contractors and consultants remain primary mitigations.
- The trend to require a university degree for entry-level cybersecurity positions is reversing. A smaller percentage of enterprises are requiring university degrees.

The number of survey respondents who believe their cybersecurity programs are appropriately funded increased to 42 percent—a five percentage-point jump and the most favorable report since ISACA began its state of cybersecurity reporting. Last year's declining optimism about cybersecurity budgets reversed course this year, with 55 percent of respondents expecting an increase in funding.

Although 82 percent of respondents believe their leadership team sees value in conducting a cyberrisk assessment, only 41 percent of respondent enterprises perform an annual cyberrisk assessment.

Despite the high-profile media attention to ransomware attacks during this reporting cycle, cyberattack reporting is mostly unchanged from last year.

Survey Methodology

In the final quarter of 2021, 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 2,031 respondents completed the survey in its entirely, and their responses are included in the results.[1]

The survey, which uses multiple-choice and Likert-scale formats, is organized into seven major sections:

- Staffing
- Skills
- Cybersecurity budgets
- Cybersecurity threats
- Cybermaturity
- Cyberrisk measurement
- Organizational governance

The survey target population includes individuals who have cybersecurity job responsibilities. Of the 2,031 respondents, 976 indicate that cybersecurity is their primary professional area of responsibility.

Figure 1 shows demographic information about the respondents, who hail from 109 countries and territories. **Figure 2** further illustrates the breadth of survey input, showing that respondents represent more than 17 industries.

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, consistent with prior-year survey reports. Result percentages are rounded to the nearest integer.

FIGURE 1—RESPONDENT DEMOGRAPHICS

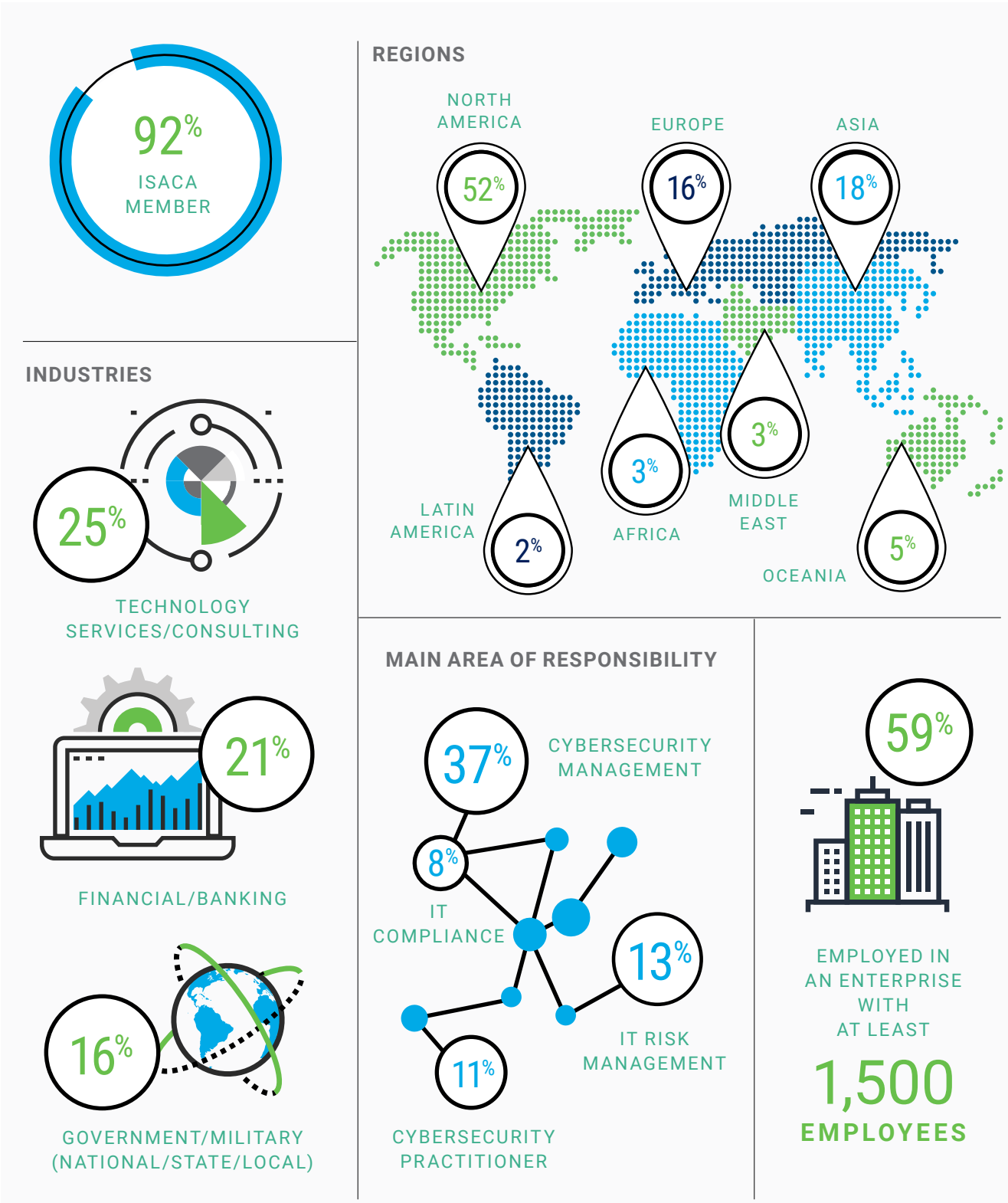
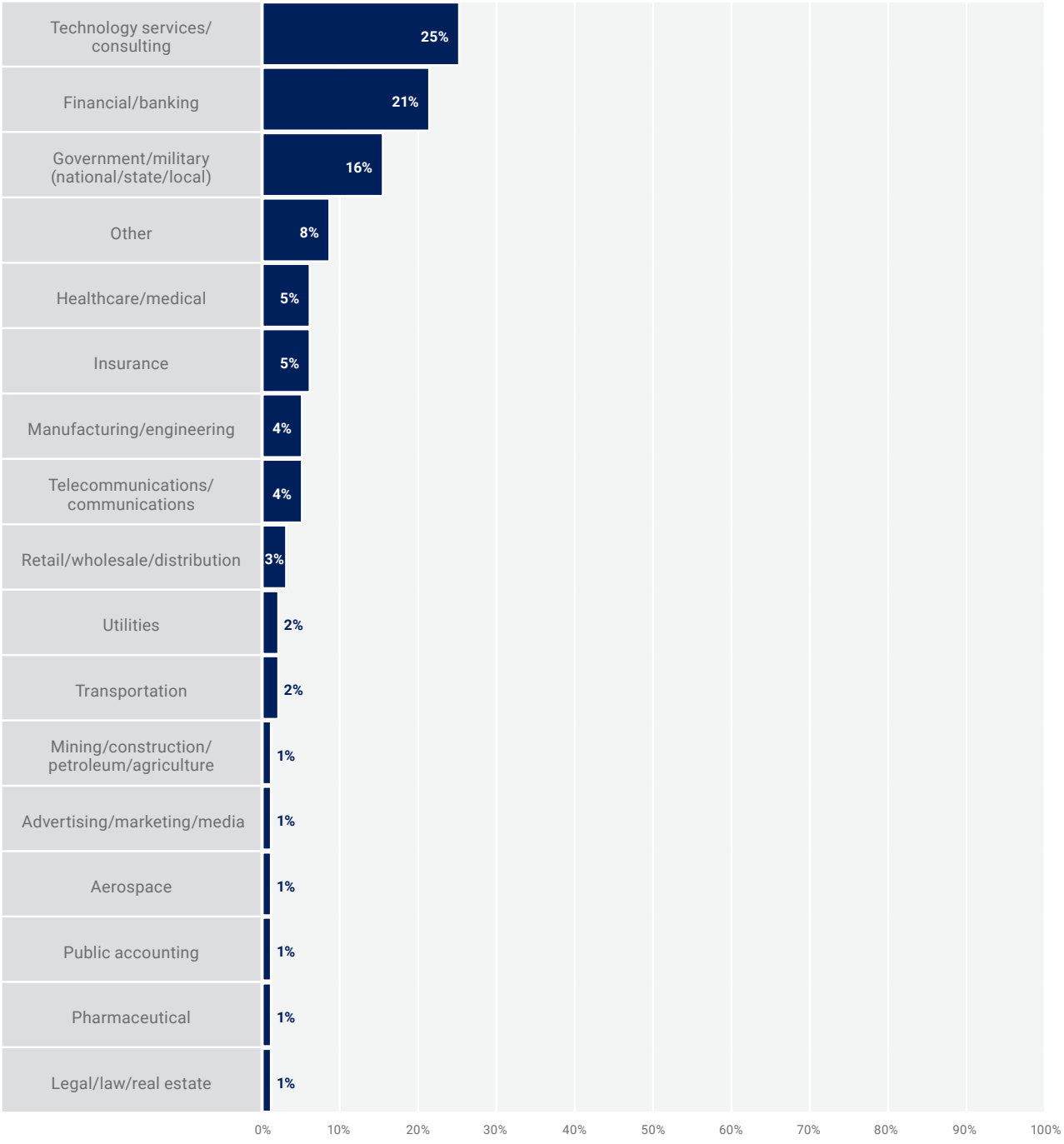


FIGURE 2—INDUSTRIES REPRESENTED

Please indicate your organization's primary industry.



Lingering Global Pandemic Affects Staffing

Multinational enterprises and small businesses across the globe encountered numerous adversities with the onset of the COVID-19 pandemic. Still, there was an underlying theme of confidence, perseverance and flexibility last year, reflected in the ISACA *State of Cybersecurity 2021* report. Business leaders in every region and industry were forced to think and execute differently, and innovation blossomed. Enterprises whose leaders balked at remote work prior to the pandemic had to change their position to stay in business and remain profitable. Morale and productivity increased. However, those early benefits are now fading as the world enters the third year of the pandemic.

There is currently an atmosphere of tension between enterprises that want to return to prepandemic norms and employees who want to hold onto newfound flexibility. Although remote work became more prevalent—largely out of necessity—many enterprises are now requiring employees to make more use of their office workspaces.[2]

The ongoing struggle between employers and employees is influencing staffing levels. In 2021, employees began leaving their jobs in droves, a trend that became known in the US as the Great Resignation. The desire for a better work-life balance is one of the factors influencing the trend, and employees in other parts of the world—including Germany, Japan and China—are also shedding jobs that demand more than they're willing to give. Labor shortages in the UK have become acute.[3]

Although ISACA's *State of Cybersecurity Survey* data focus on the cybersecurity profession, the power struggle between business leaders and workers has had a widespread influence on the technology and healthcare industries overall.[4] Flexible work expectations increased due to the pandemic and have become weighty considerations when employees evaluate potential career moves.[5] In 2021, employees pushed back against mandates to return to a physical office space, resulting in many enterprises revising or curtailing plans to return to in-office work.[6] This issue and high-wage expectations have led to an intense battle for talent.[7] The ISACA *State of Cybersecurity Survey* responses confirm this struggle—60 percent of respondent enterprises experienced difficulties retaining qualified cybersecurity professionals in 2021, which is a seven-percentage-point increase from 2020 (53 percent).

Only 44 percent of ISACA survey respondents manage security staff with less than three years of work experience. The workforce pipeline challenges with placing sufficient entry-level cyberprofessionals strain an aging workforce. Sixty-five percent of survey respondents are between ages 35 and 54; the largest percentage of respondents (35 percent) are between

2 (ISC)²®, "A Resilient Cybersecurity Profession Charts the Path Forward: (ISC)² Cybersecurity Workforce Study, 2021," www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

3 Hancock, T.; "Lie Flat Meets the Great Resignation," Bloomberg, 8 December 2021, www.bloomberg.com/news/newsletters/2021-12-08/what-s-happening-in-the-world-economy-lie-flat-meets-great-resignation

4 Cook, I.; "Who Is Driving the Great Resignation?" *The Harvard Review*, 15 September 2021, https://hbr.org/2021/09/who-is-driving-the-great-resignation

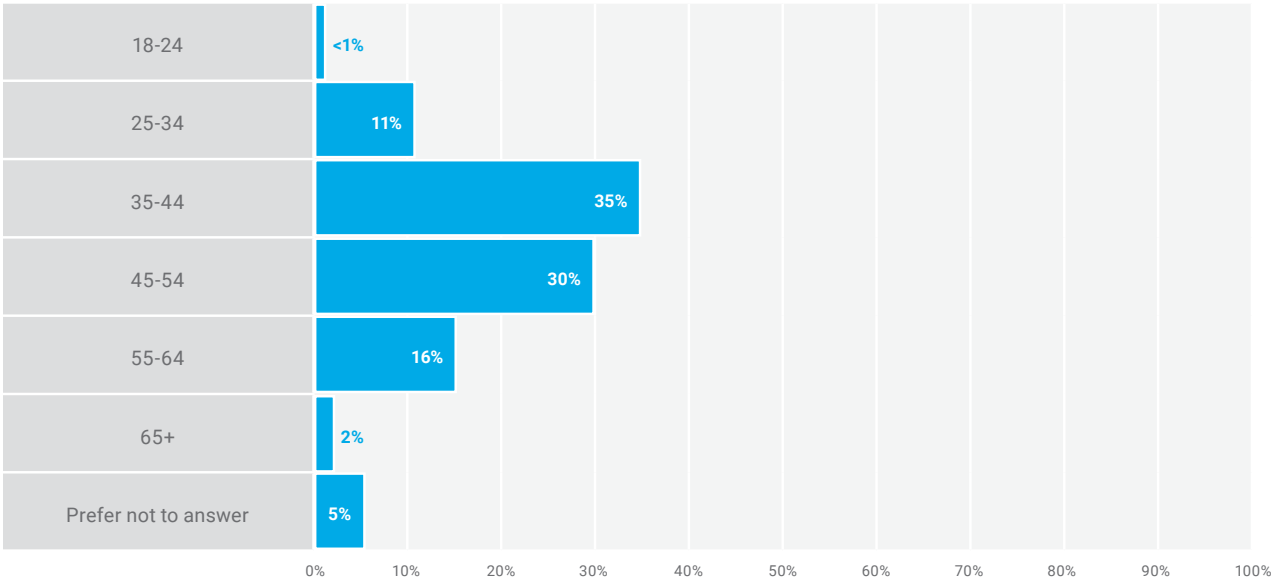
5 Venkataramani, S.; "Returning Employees to an Office? Consider the Talent Risks," 3 June 2021, www.gartner.com/smarterwithgartner/returning-employees-to-an-office-consider-the-talent-risks

6 Johnston, K.; "Workers Are Resisting Being Called Back to the Office—and Some Employers Are Scrapping Their Plans," The Boston Globe, 18 November 2021, www.bostonglobe.com/2021/11/18/business/workers-are-resisting-being-called-back-office-some-employers-are-scrapping-their-plans/

7 WTW, "Difficulty Hiring and Keeping Workers Will Last Into 2022, Willis Towers Watson Survey Finds," 25 August 2021, www.wtwco.com/en-US/News/2021/08/difficulty-hiring-and-keeping-workers-will-last-into-2022-willis-towers-watson-survey-finds

FIGURE 3—WORKFORCE BY AGE

Please select your age.



ages 35 and 44 (**figure 3**). This result is problematic because a global study reports that midcareer employees, those from age 30 to 45 years old, are driving the Great Resignation. Resignation rates of midcareer employees increased 20 percent between 2020 and 2021.[8]

This year's survey findings on current staffing nearly mirror those of last year (**figure 4**). For many years, the demand for cybersecurity talent has steadily risen and the job market remains promising for aspiring practitioners and career changers if employers heed the calls for more entry-level positions at scale. The cybersecurity industry continues to be a seller's market.[9]

Employee burnout related to the lingering pandemic and widespread reluctance to return to the office have hampered retention. Sixty percent of survey responses indicate organizations are struggling to retain talent, which is seven percentage points higher than last year. Further, multiyear data suggest that last year's results were anomalous—uncertainty early in the pandemic influenced employees to remain in place (**figure 5**).

As in previous years, the data suggest that staffing levels, retention and cyberattacks are somewhat interrelated. Sixty-nine percent of respondents whose organizations experienced more cyberattacks in the past year report being somewhat or significantly understaffed. Similarly, 70 percent of respondents whose organizations experienced more attacks indicate their employers experienced difficulties retaining qualified cybersecurity professionals, up seven percentage points from last year.

As in previous years, the data suggest that staffing levels, retention and cyberattacks are somewhat interrelated.

Additionally, 73 percent of respondents whose cybersecurity teams are significantly understaffed say their organizations experienced difficulties retaining qualified cybersecurity professionals. This is an increase of eight percentage points from last year and is conceivably due to burnout related to the lingering pandemic.

8 *Op cit* Cook

9 Sellers are the cybersecurity job applicants (or employees); buyers are the hiring enterprises that are seeking qualified candidates.

FIGURE 4—CYBERSECURITY STAFFING

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

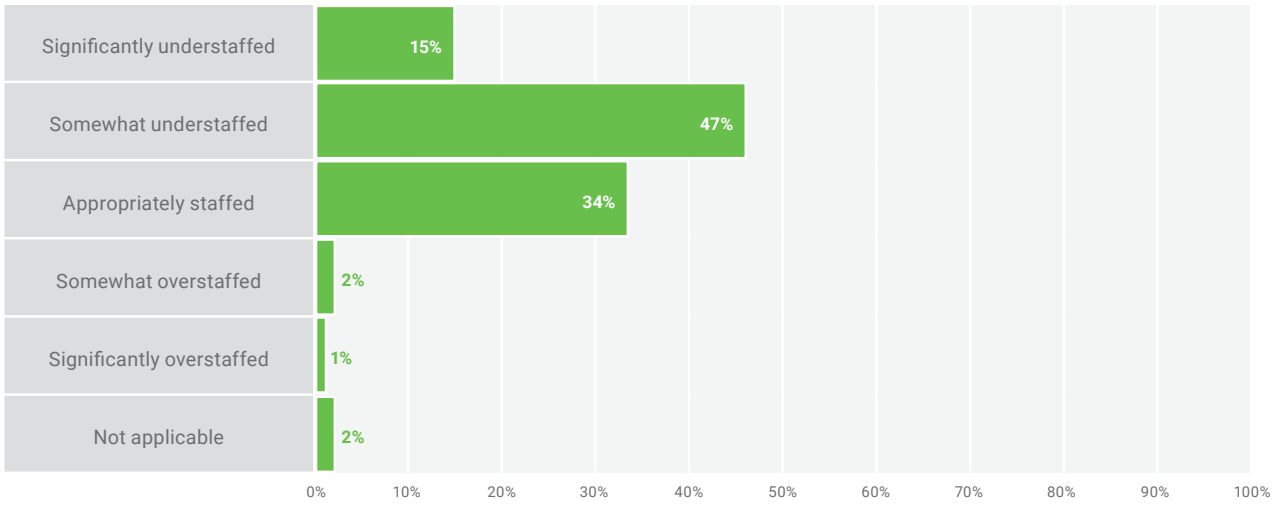


FIGURE 5—RETENTION DIFFICULTIES (2019-2022)

Has your organization experienced difficulties retaining qualified cybersecurity professionals?

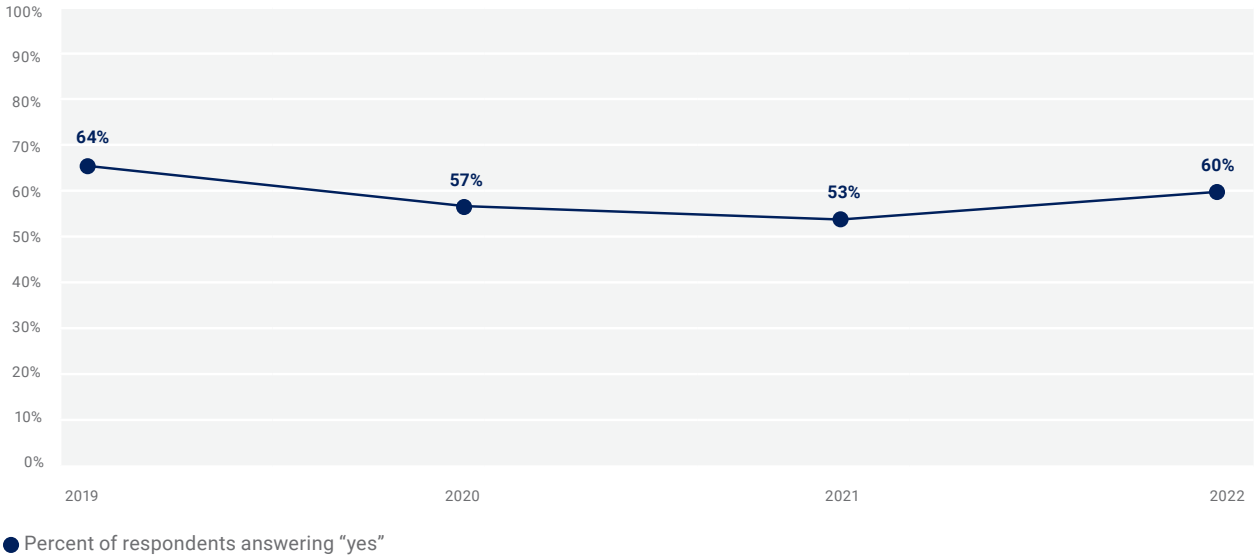
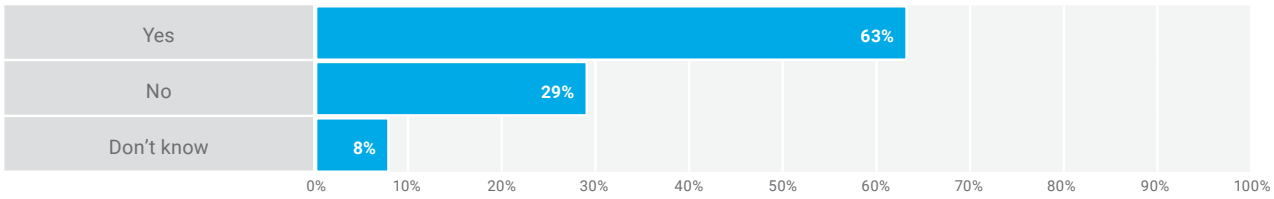


FIGURE 6—UNFILLED POSITIONS

Does your organization have unfilled (open) cybersecurity positions?

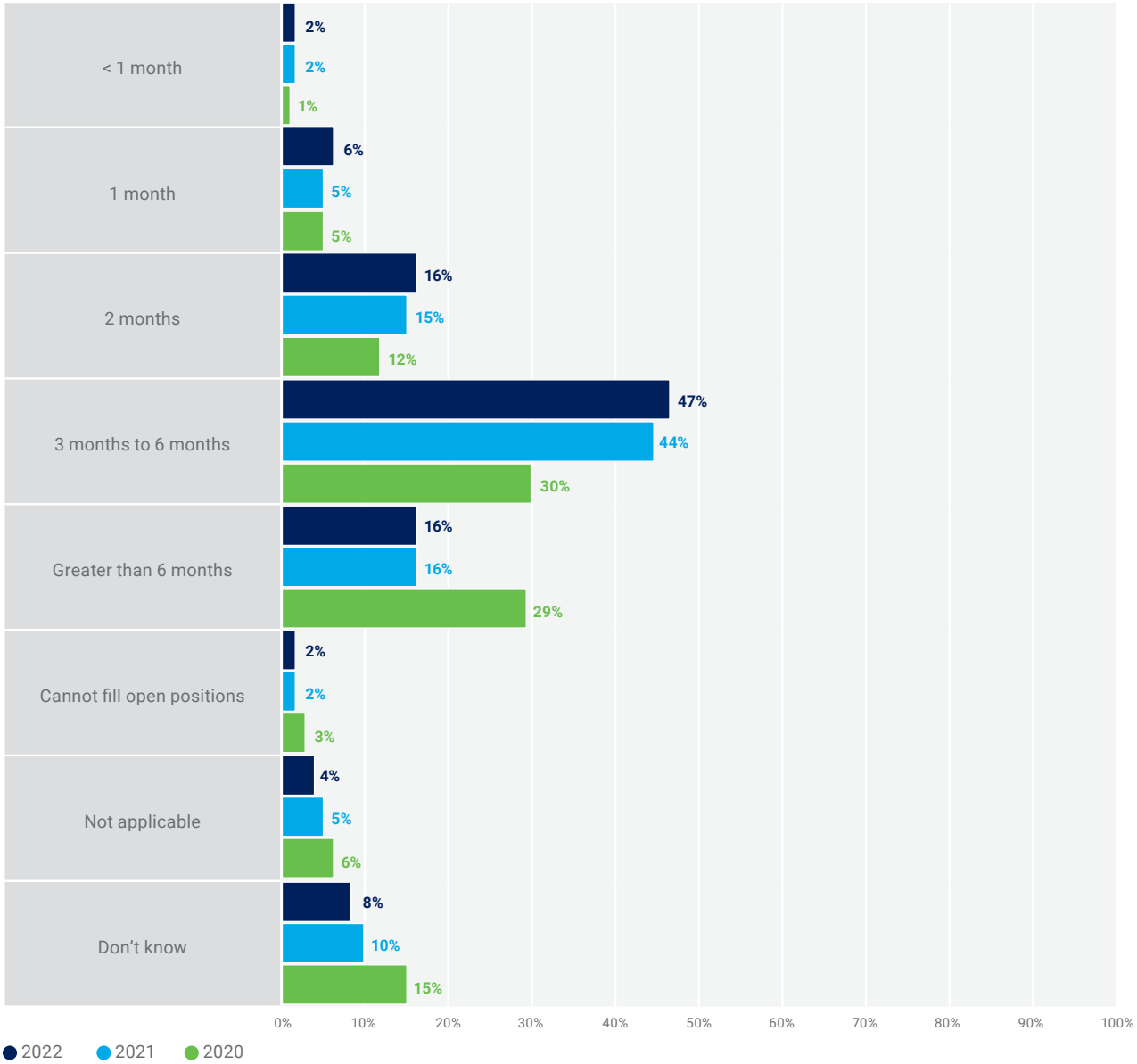


Vacancies

Sixty-three percent of survey respondents claim their organizations have unfilled cybersecurity positions (**figure 6**), which represents an eight percentage-point increase from last year's data (55 percent). The survey results indicate a modest improvement in the amount of time required to fill a cybersecurity position (**figure 7**), with a five percentage-point increase in the percent of respondents whose organizations take less than six months to fill vacant positions.

FIGURE 7—TIME TO FILL A CYBERSECURITY POSITION (2020-2022)

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



Technical cybersecurity positions remain the top vacancy again this year (**figure 8**). For managers and directors who are exploring new opportunities, the survey data echo last year's positive finding of the largest increase in vacancies at the executive or C-suite level since 2019. Year-over-year data on unfilled positions are illustrated in **figure 9**.

With regard to future demand (**figure 10**), respondents expect slightly higher growth across each of the five categories of positions, compared to last year survey results. **Figure 11** shows five-year trending on future demand, which overturns last year's indication of a leveling off in hiring demands.

FIGURE 8—PERCENTAGES OF UNFILLED POSITIONS AT GIVEN ORGANIZATIONAL LEVELS

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

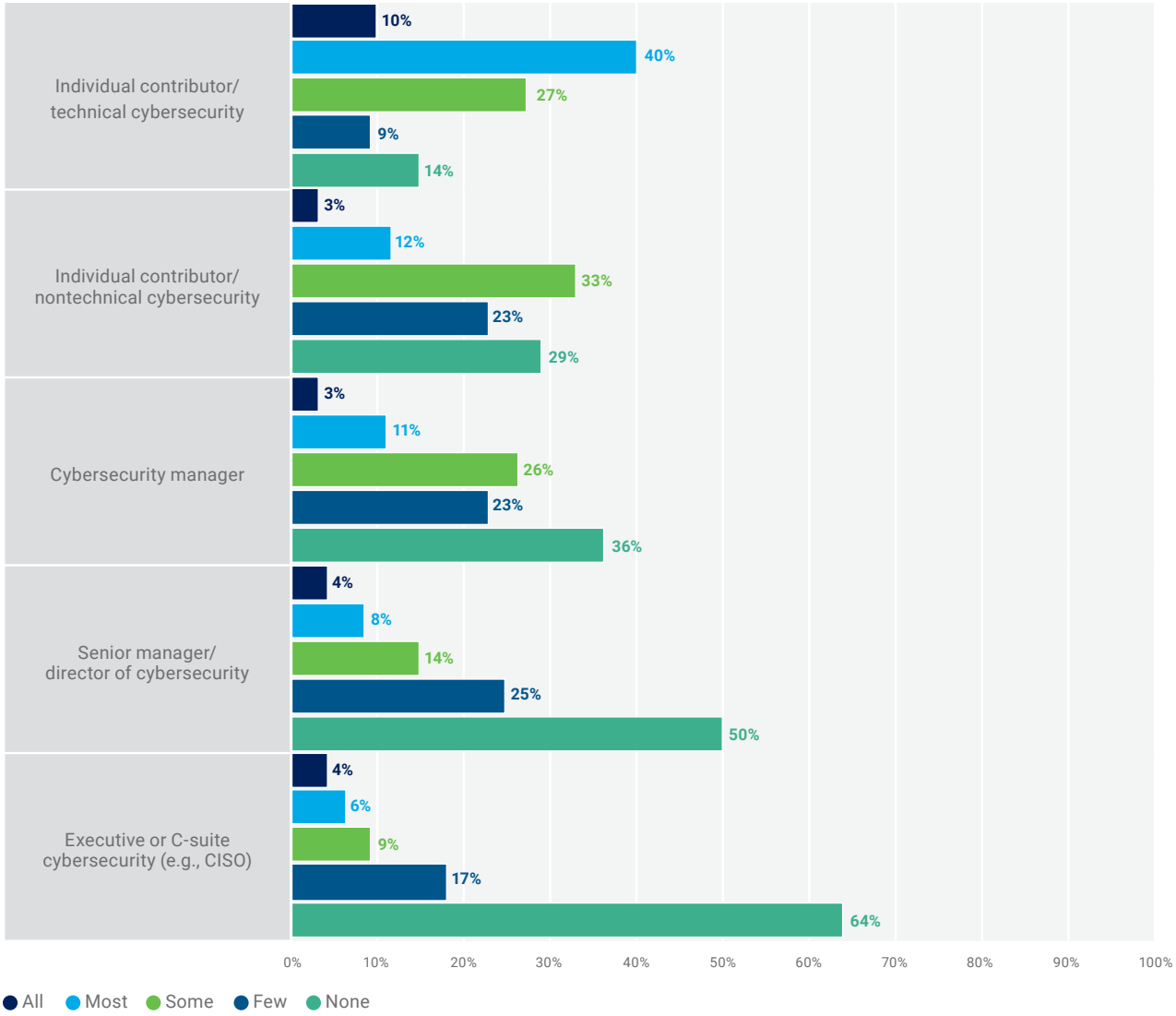
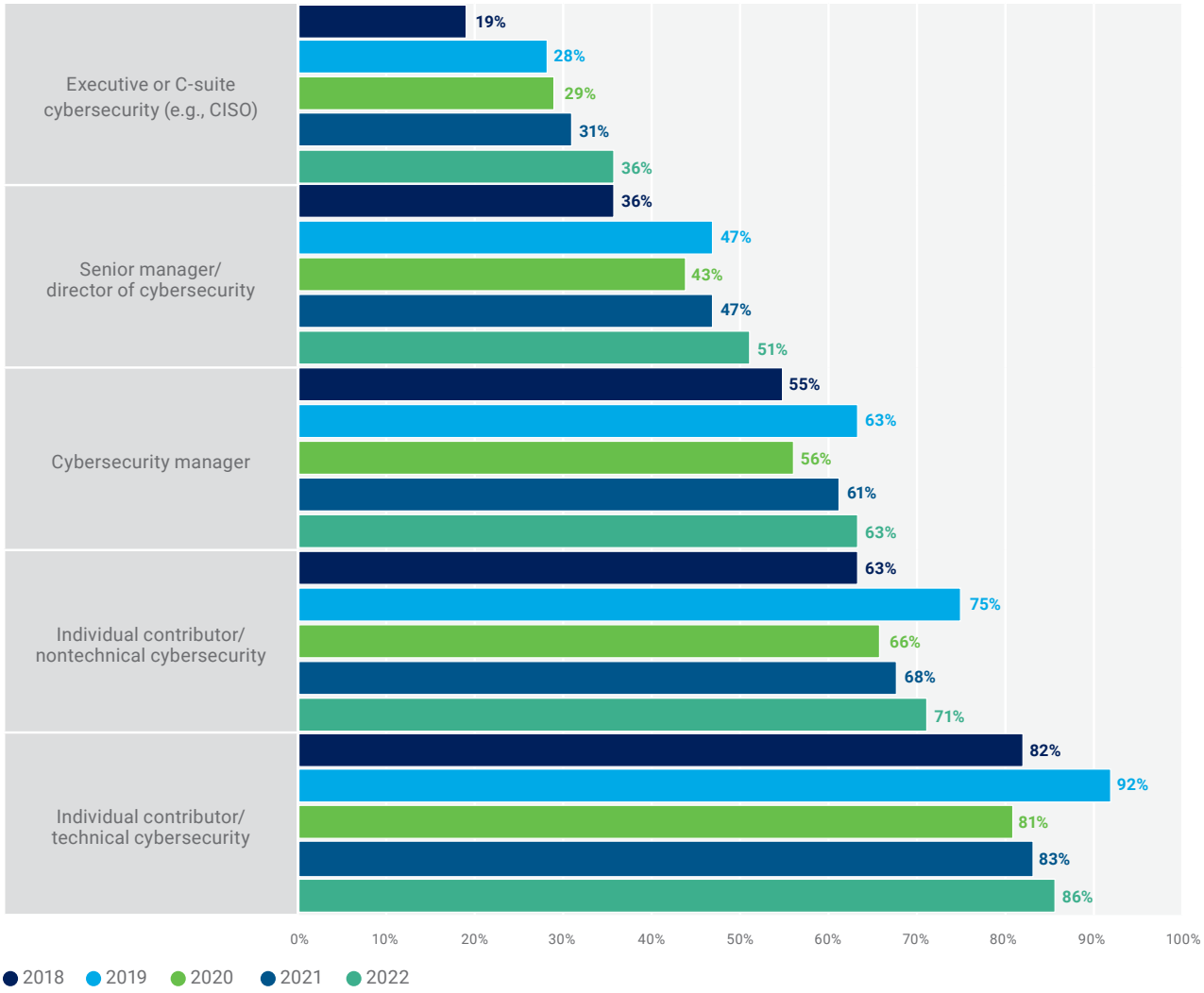
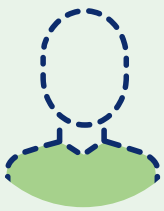


FIGURE 9—UNFILLED POSITION REPORTING (2018-2022)[10]





Technical cybersecurity positions remain the top vacancy again this year. For managers and directors who are exploring new opportunities, the survey data echo last year's positive finding of the largest increase in vacancies at the executive or C-suite level since 2019.

10 This figure compares reported unfilled position data for 2018 to 2022 *State of Cybersecurity* reports. Percentages represent the sum of all reported vacancy percentages for each position and exclude the "None" responses.

FIGURE 10—FUTURE HIRING DEMAND

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

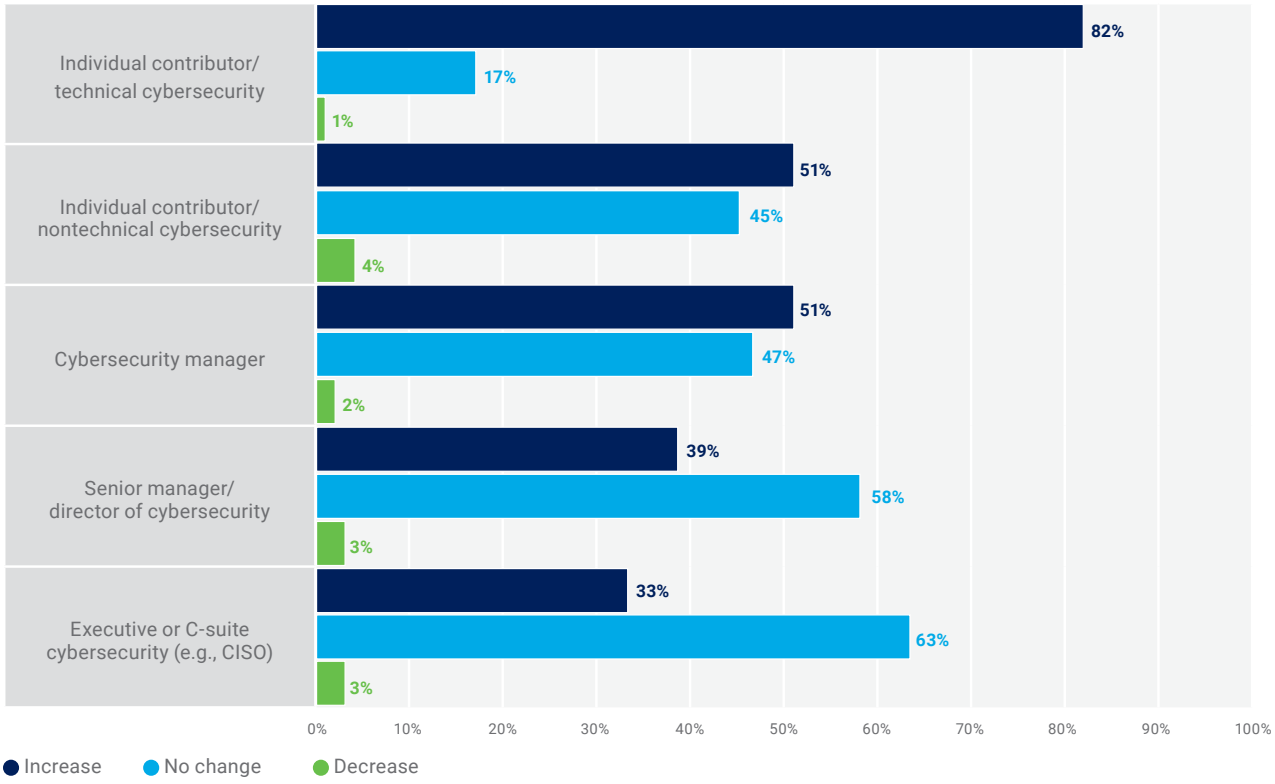
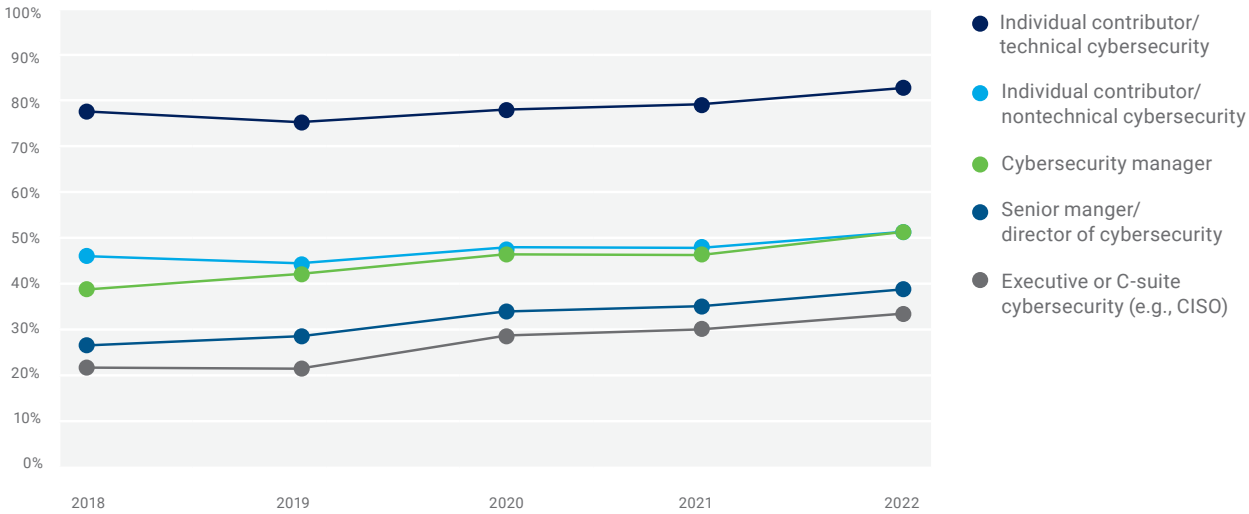


FIGURE 11—HIRING DEMAND TRENDING (2018-2022)



Pipeline Challenges

Survey data support previous reporting that hiring managers have low confidence in cybersecurity applicants' qualifications. **Figure 12** shows that 55 percent of those surveyed generally do not believe applicants are well qualified.

Among those who regard fewer than half of applicants as well qualified, 53 percent report the average time to fill an open position as three to six months; among those who regard more than half of applicants as well qualified, 50 percent of respondents report the same average duration to fill an open position—i.e., three to six months.

Among hiring managers with more favorable opinions of applicants' qualifications, 38 percent report no meaningful difference in the time to fill positions; among hiring managers with less favorable views of applicants' qualifications, 39 percent—just one additional percentage point—report no meaningful difference in the time to fill positions.

Thus, hiring managers' general attitudes toward applicants' qualifications do not correlate to significant statistical differences in the time enterprises spend filling positions.

Figure 13 shows that prior hands-on cybersecurity experience remains the primary factor (73 percent) in determining whether a candidate is considered qualified. The largest skill gap continues to be soft skills (**figure 14**).

In this year's survey, cloud computing is an addition to the list of skill gaps available for respondents' selection (**figure 14**). Survey responses indicate that cloud computing is the second-largest skill gap among cybersecurity professionals (52 percent), just behind soft skills—the top skill gap identified (54 percent). Other notable gaps include security controls implementation, coding, software development-related topics (e.g., languages, machine code, testing, deployment), data-related topics (e.g., characteristics, classification, collection, processing, structure) and networking-related topics (e.g., architecture, addressing, networking components).

FIGURE 12—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?

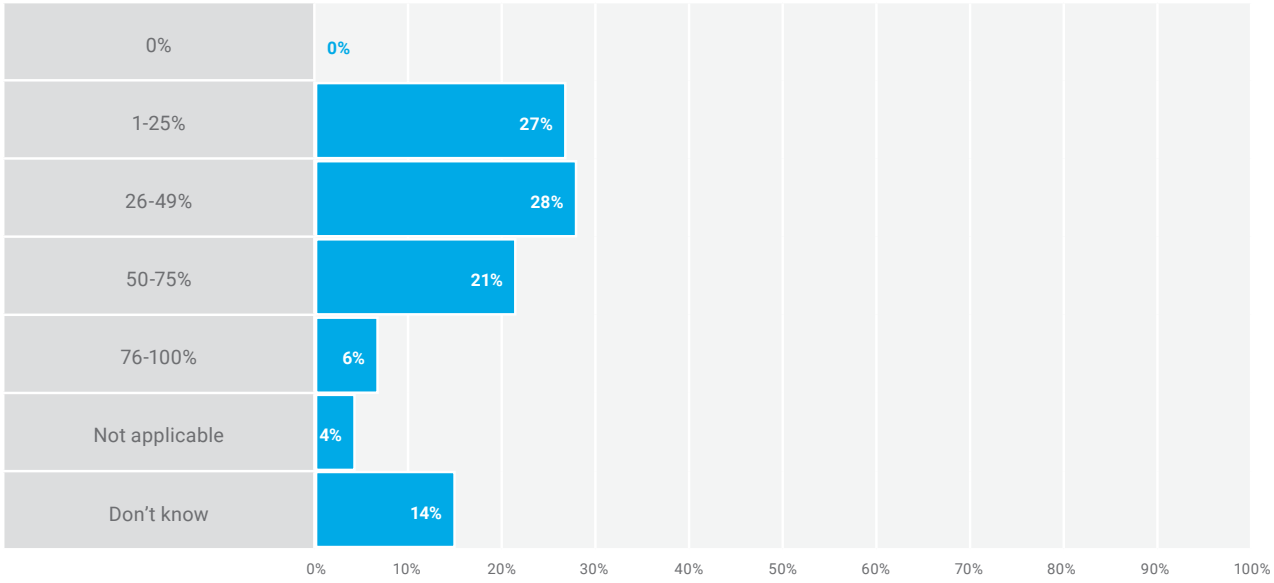
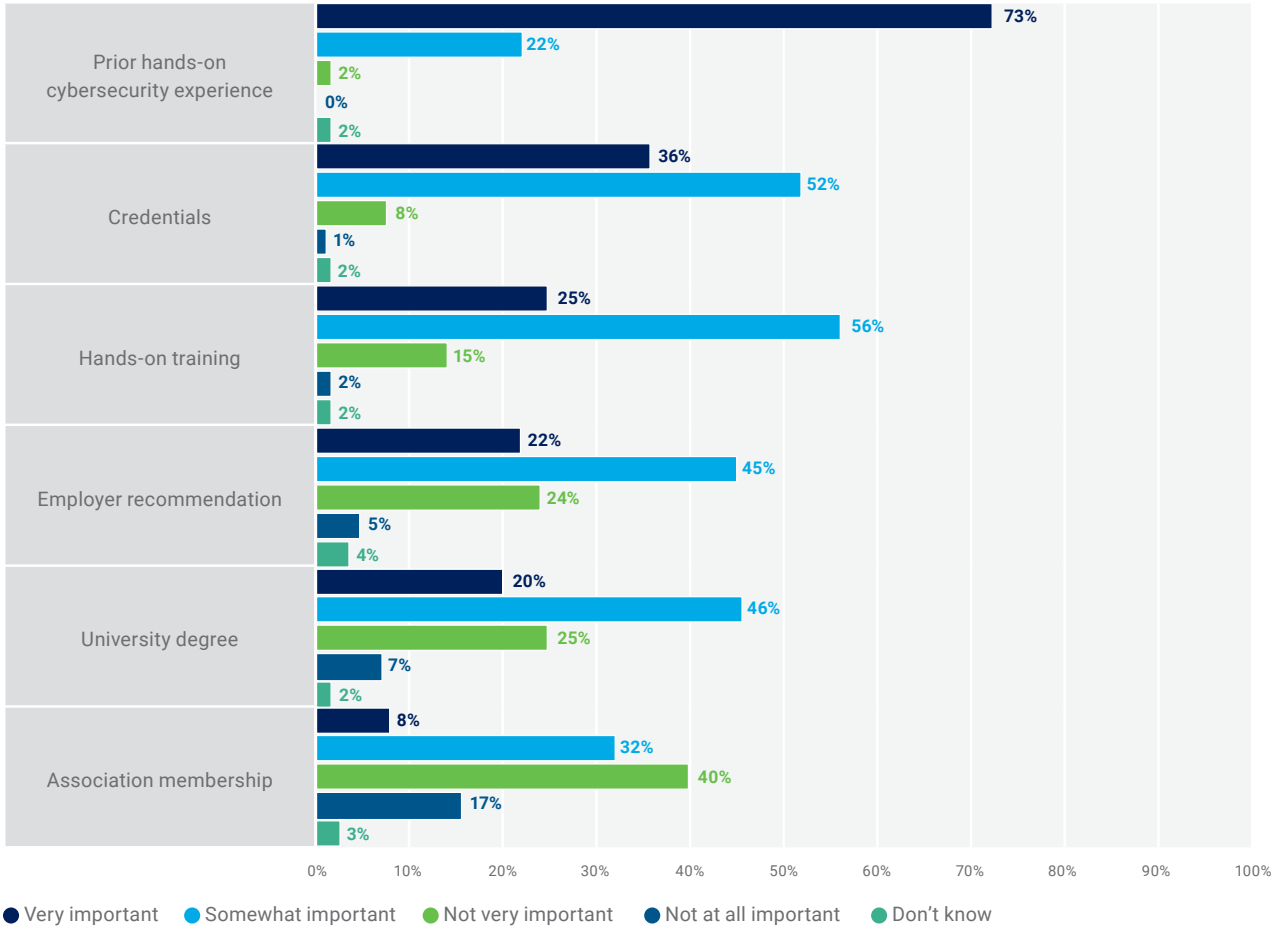


FIGURE 13—CANDIDATE QUALIFICATIONS

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

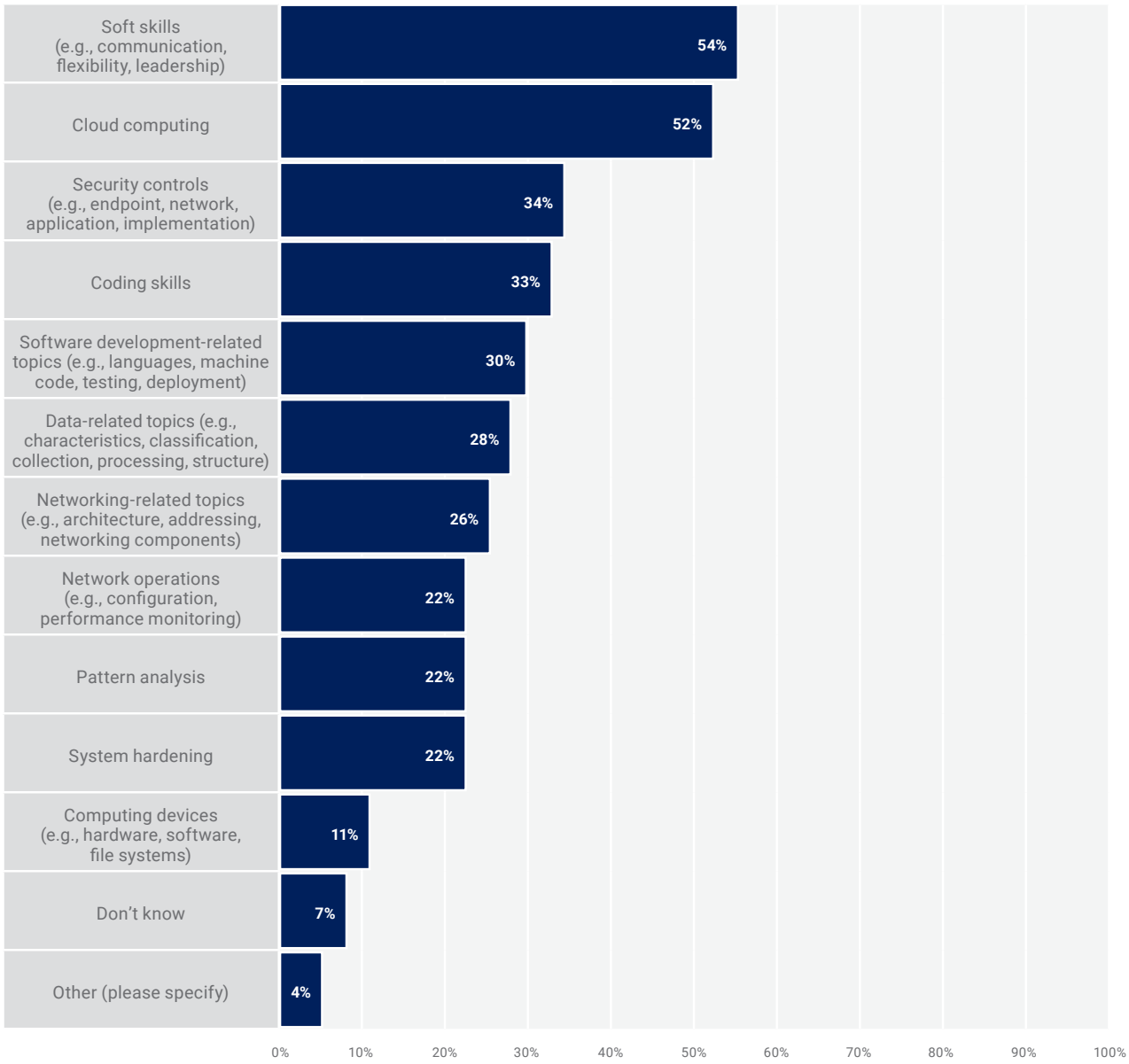


Survey responses indicate that cloud computing is the second-largest skill gap among cybersecurity professionals, just behind soft skills—the top skill gap identified.

Other notable gaps include security controls implementation, coding, software development, data-related topics and networking-related topics.

FIGURE 14—QUANTIFIED SKILL GAPS

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



University Insights

Universities remain the primary source for supplying the talent pipeline. Survey respondent opinions continue to be split on whether recent graduates with a university degree are well prepared for the cybersecurity challenges facing enterprises (**figure 15**). However, university degrees appear to be losing favor, with only 52 percent of organizations requiring a degree to fill entry-level cybersecurity positions—a six percentage-point decrease from last year's data (**figure 16**).

Most geographic areas report a decline in organizations requiring a university degree, with the largest drop reported in the Middle East and Oceania. This trend is a change from last year, when report data indicated that the trend toward requiring a university degree was increasing. **Figure 17** shows, by region, the percentage of enterprises that require

a university degree for entry-level cybersecurity positions, based on 2021 and 2022 survey data, and indicates the direction of the trend in each region.

As for skill gaps among recent university graduates, the survey responses highlight soft skills again this year (**figure 18**) as the area of greatest concern. However, most of the technical skills listed show a decreasing gap from prior-year data (**figure 18**), suggesting slight improvements in technical skills among recent graduates.

With respect to their beliefs about graduate preparedness for organizational challenges, there is a significant difference between respondents from organizations requiring a university degree for entry-level positions and respondents from organizations that do not require a university degree for entry-level positions. Among those whose organizations typically require a university degree for entry-level positions, 33 percent either strongly agree or agree that recent university graduates in cybersecurity are well prepared for the challenges in their organization. Only 23 percent of those whose organizations do not require university degrees for entry-level positions either strongly agree or agree that recent cybersecurity graduates are well prepared.

FIGURE 15—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?

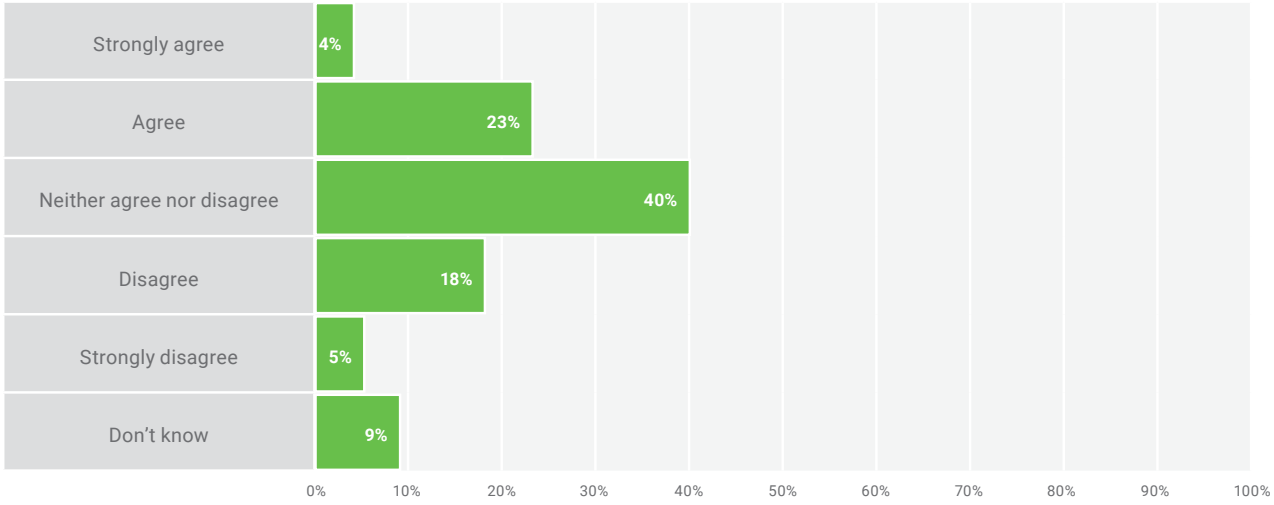


FIGURE 16—UNIVERSITY REQUIREMENT

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

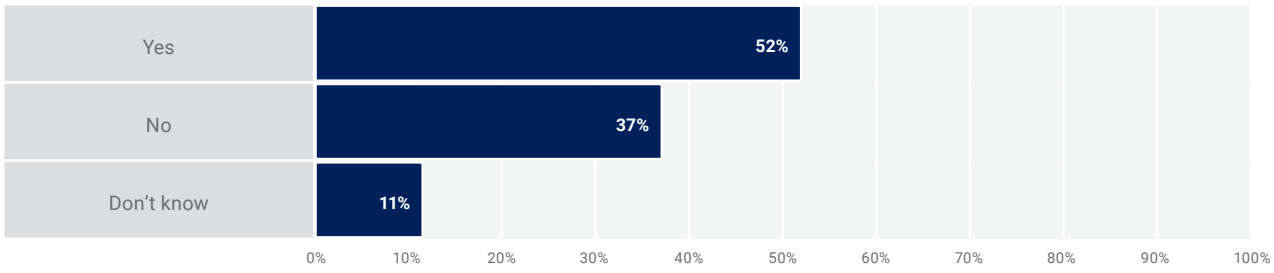
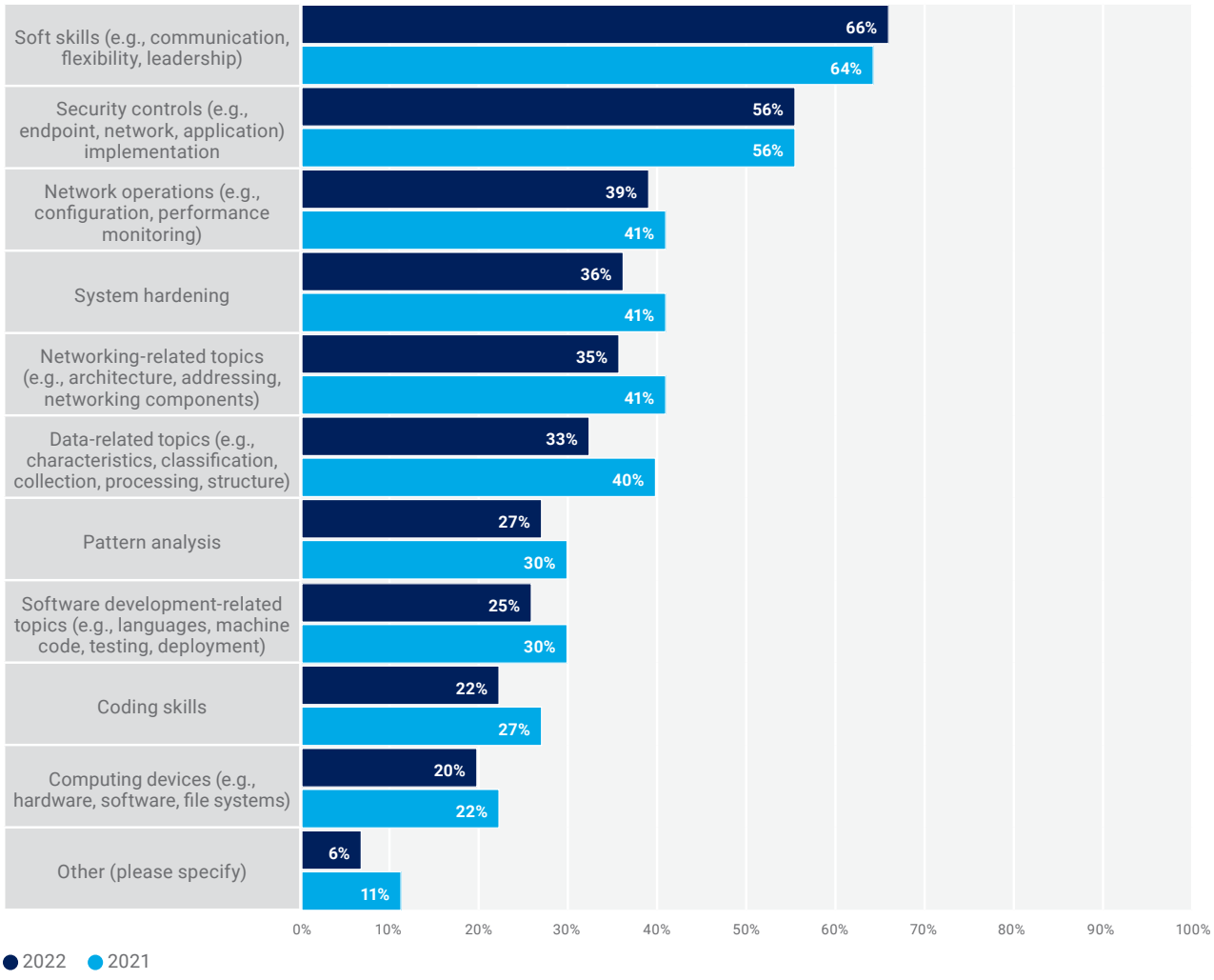


FIGURE 17—ENTRY-LEVEL DEGREE REQUIRED—PERCENTAGES BY REGION (2021-2022)

REGION	2021	2022	TREND
Asia	68	68	→
Africa	69	71	↑
Europe	51	45	↓
Latin America	68	61	↓
North America	54	49	↓
Middle East	78	59	↓
Oceania	41	27	↓

FIGURE 18—SKILLS GAPS AMONG RECENT GRADUATES

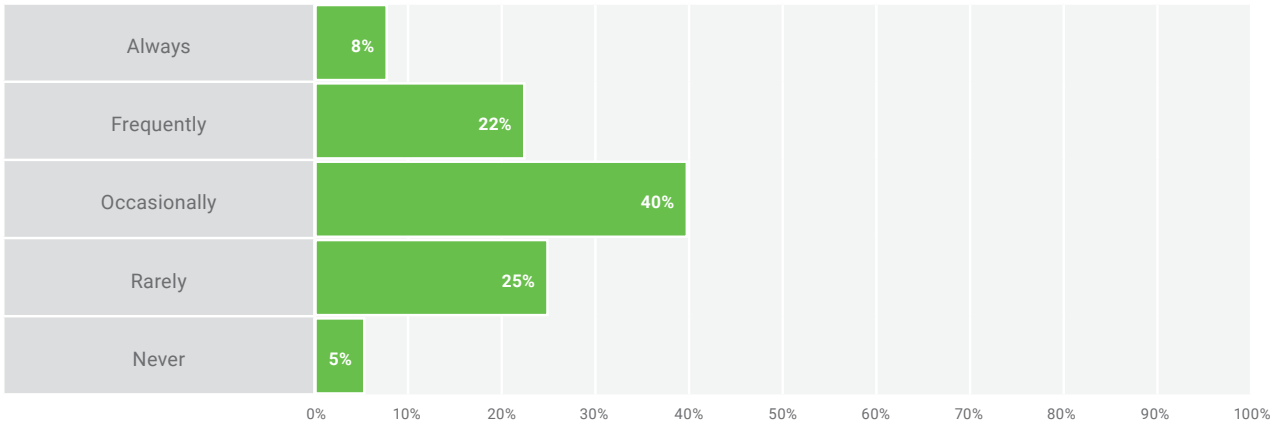
Which of the following skills gaps have you noticed among recent university graduates?



Recruitment remains a challenge for many enterprises. Survey data shown in **figure 19** highlight the ongoing mismatch between hiring managers and their human resources (HR) recruitment efforts, largely consistent with last year's findings. Shortening the time to fill open positions may depend on closing this gap. Of the respondents who say HR always or frequently understands their cybersecurity hiring needs, 35 percent report filling open positions takes two months or less, an increase from last year's 30 percent.

FIGURE 19—COMPREHENSION OF HIRING NEEDS BY HR

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



Retention Challenges

Although the 2021 ISACA report data indicated an improvement in employee retention, this year's data indicate a reversal of those improvements. Sixty percent of survey responses point to difficulty with retaining talent—a seven percentage-point increase from last year. However, some change is evident in the factors survey respondents view as instrumental in cybersecurity professionals' decisions to leave their positions (**figure 20**).

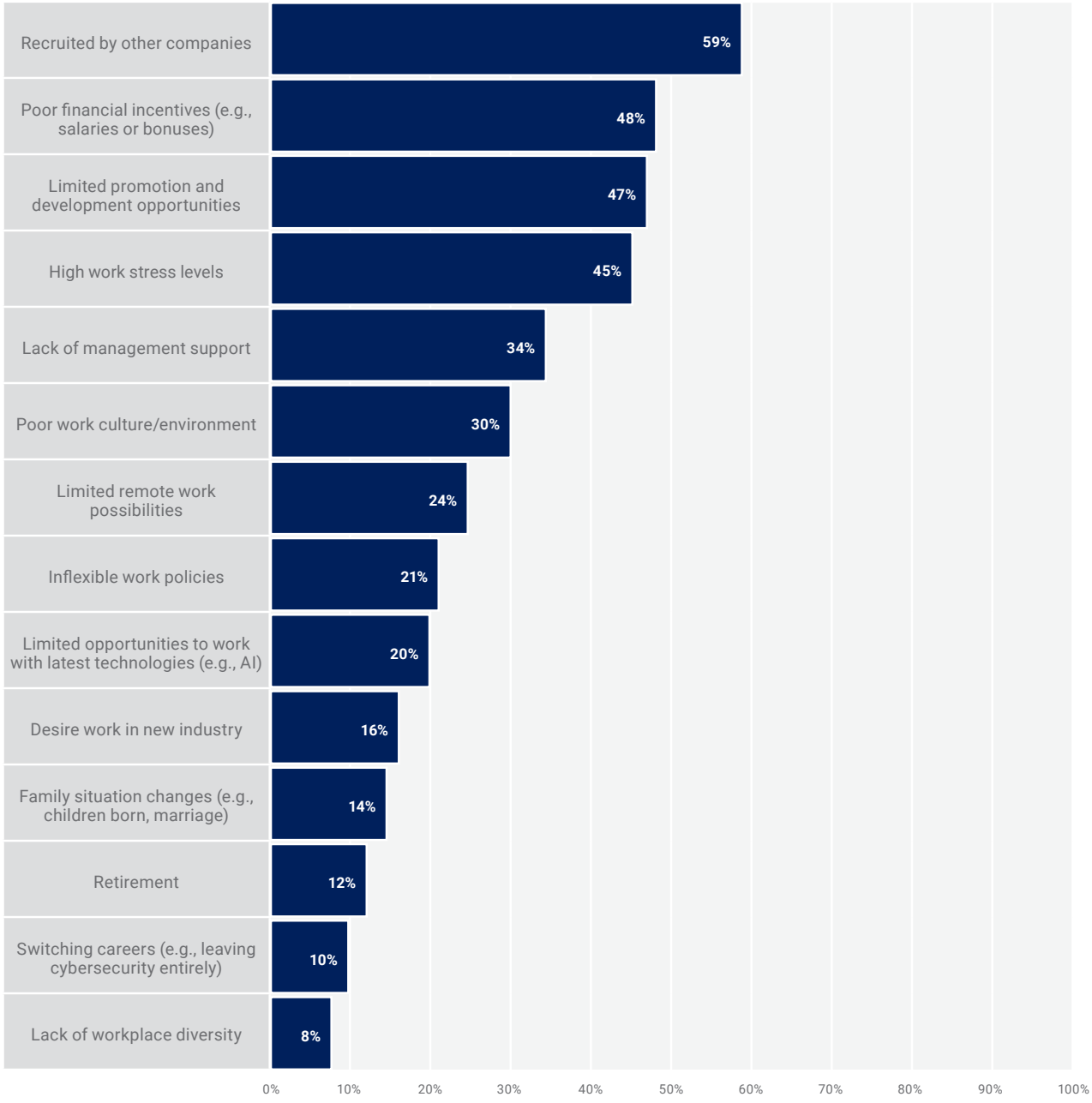
Forty-five percent of this year's respondents say high work stress levels is a contributing factor, compared with 42 percent last year. Workplace stress may be a consequence of multiple factors, including difficulty in retaining staff, disclosure of high-profile vulnerabilities, an indiscriminate and dynamic threat landscape, and supply chain compromises.

Some employers' requirements that employees return to offices may underly the increases in this year's survey of limited remote work possibilities and inflexible work policies as factors that contribute to quitting. The percentage of respondents indicating retirement as a reason for departure remained static from last year, which may indicate that lucrative benefits packages are tempting some employees to join other organizations instead of retiring.

Although the 2021 ISACA report data indicated an improvement in employee retention, this year's data indicate a reversal of those improvements.

FIGURE 20—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?

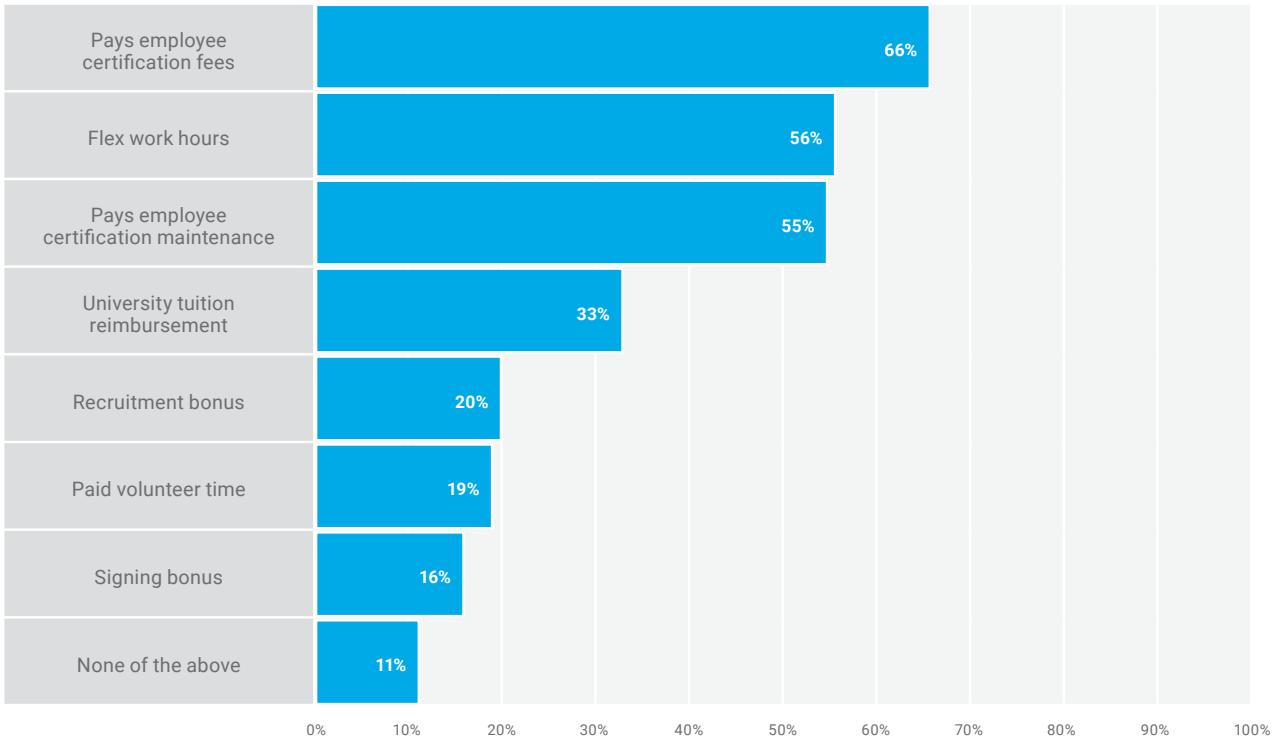


Employer Benefits

New to this year's report are responses concerning organizational benefits. Competitive benefits can positively influence employee retention. Sixty-six percent of respondents indicate their employers pay employee certification fees, and 55 percent of respondent employers pay certification maintenance (e.g., renewal) fees. These benefits provide opportunities for employees to acquire and maintain credentials that cybersecurity job postings often highlight as required or desired. Fifty-six percent of respondents report their employers offer a flexible work schedule (**figure 21**).

FIGURE 21—EMPLOYER BENEFITS

Which of the following benefits does your employer offer? Select all that apply.



Qualifying Workforce Issues

This year's survey addresses specific skill issues affecting the cybersecurity workforce. When asked to select the most important security skills their organizations need today, 52 percent of respondents place cloud computing (**figure 22**) in their top five lists. Communication (both listening and speaking) is the top soft skill security professionals need in their organizations, according to 57 percent of respondents (**figure 23**). Only 16 percent of respondents selected honesty as one of the top security skills needed in their organizations, a surprising finding considering its importance to any protection-related occupation, especially cybersecurity. If this low number is an indication that honesty is not prioritized, there may be long-term ramifications, particularly in light of 60 percent of survey respondents' belief that most organizations underreport cybercrime, even if required to do so.

Many US and UK consumers share the belief that cybercrimes are underreported, yet India and Australia consumers assume reporting is accurate due to governmental mandates, ISACA's internal research suggests.[11]

Only 16 percent of respondents selected honesty as one of the top security skills needed in their organizations, a surprising finding considering its importance to any protection-related occupation, especially cybersecurity.

11 ISACA, *Consumer Cybersecurity Research Report* (unpublished), December 2021

FIGURE 22—TOP 5 SECURITY SKILLS

Please choose the top five most important security skills needed in your organization today.

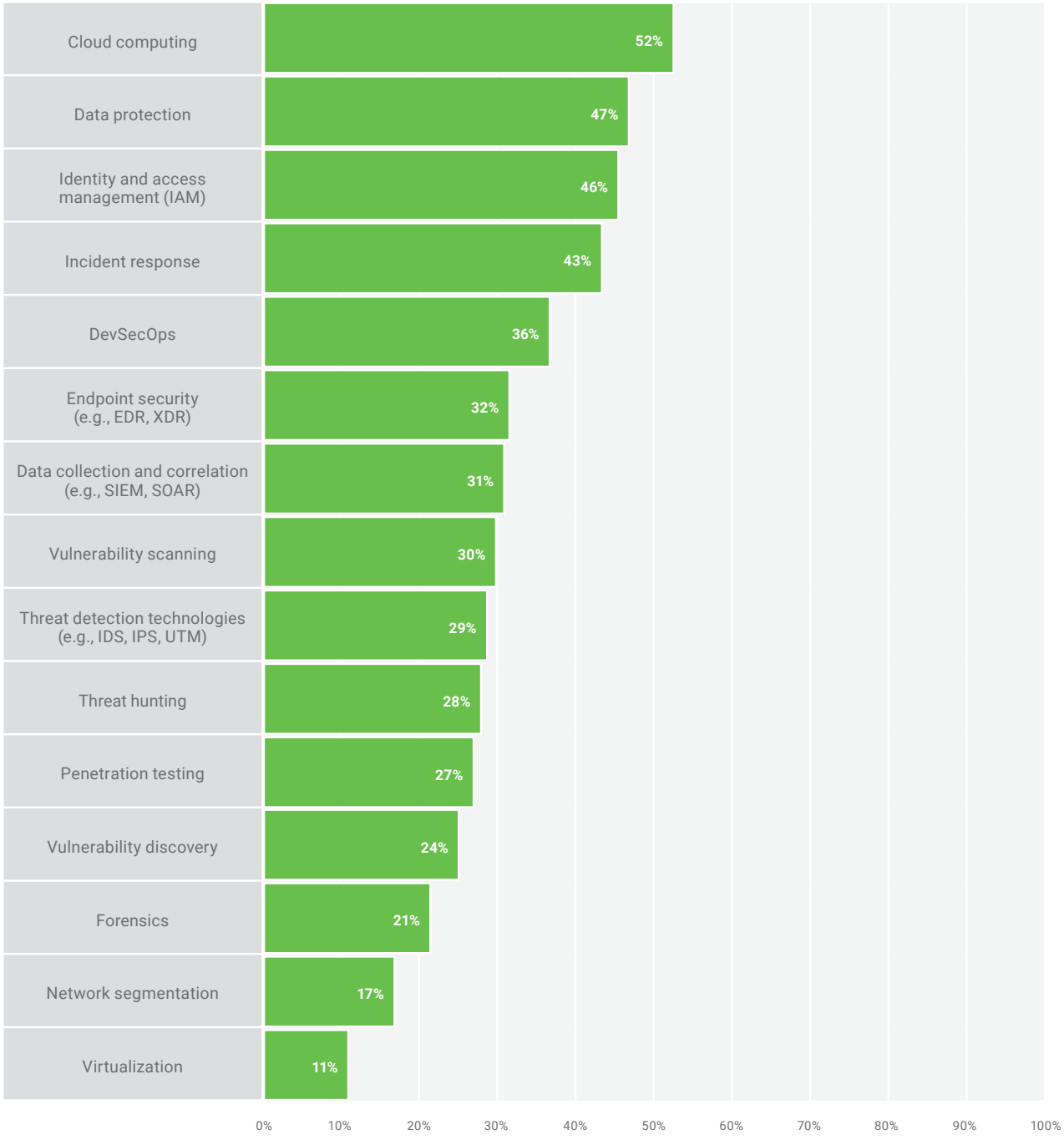
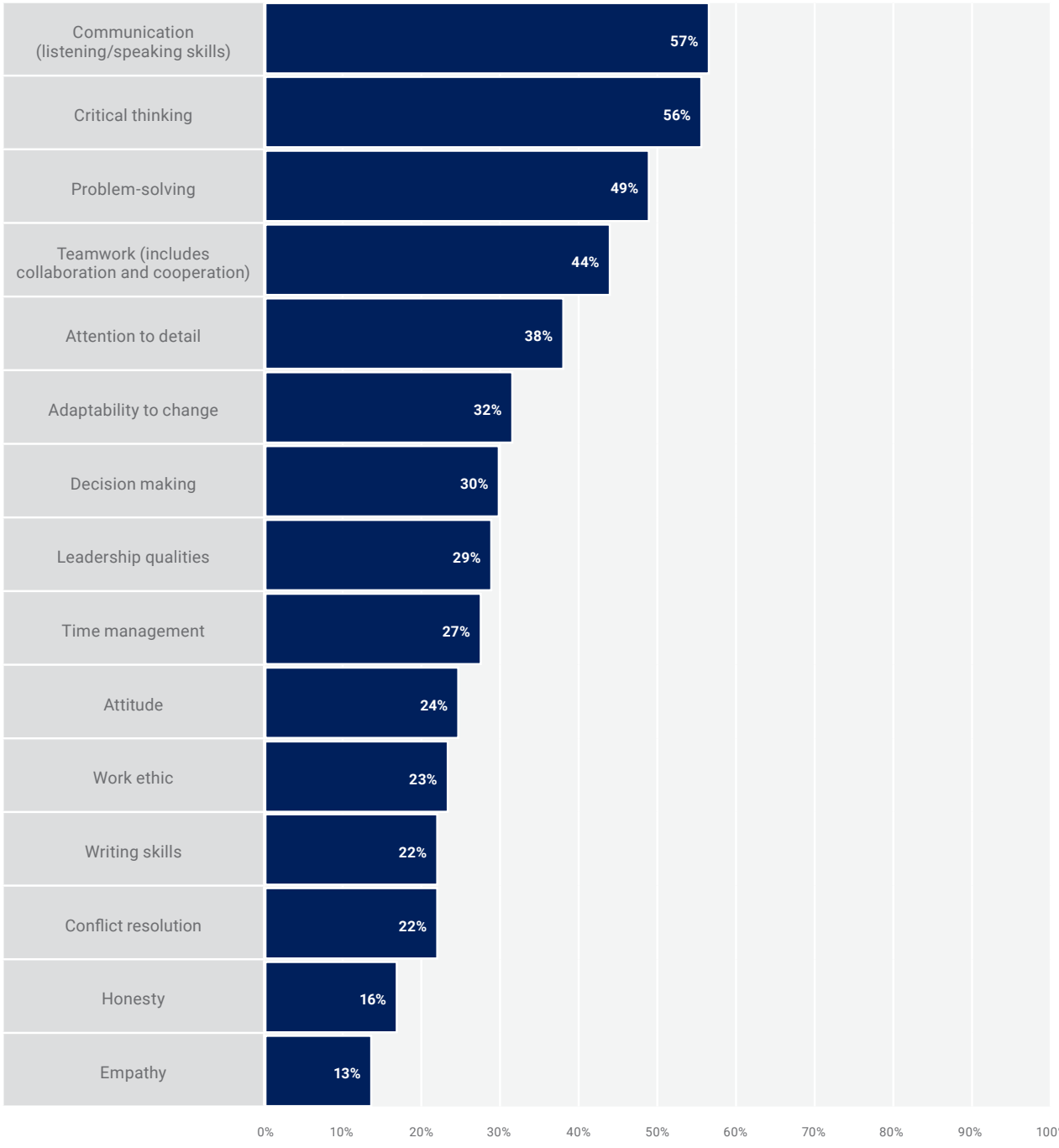


FIGURE 23—TOP 5 SOFT SKILLS

Please choose the top five most important soft skills needed by security professionals in your organization today.

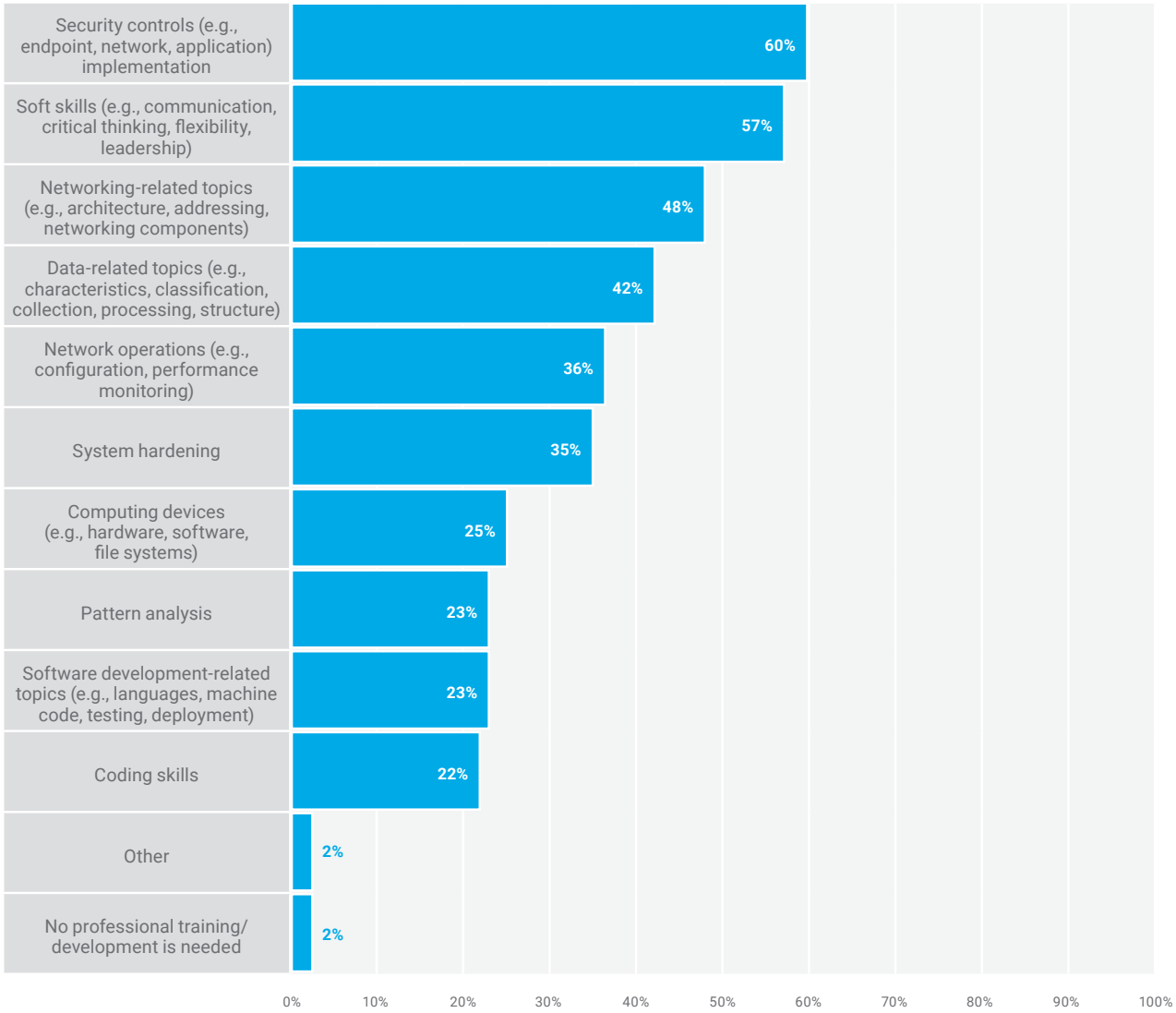


Early Career Staff Insights

Another new topic in this year's ISACA *State of Cybersecurity Survey* concerns the professional development needs of security staff with less than three years of work experience. Six in 10 respondents name security controls as one of the areas of training most needed by security staff with less than three years of work experience. Training in soft skills (e.g., communication, critical thinking and flexibility) follows closely, with 57 percent of respondents noting the need (**figure 24**).

FIGURE 24—PROFESSIONAL DEVELOPMENT NEEDS FOR STAFF WITH LESS THAN 3 YEARS EXPERIENCE

Thinking about your security staff with less than 3 years of work experience, in which of the following areas is professional development/training most needed? Select all that apply.



Human Capital Mitigations

With respect to specific actions employers have taken to address skill gaps, responses this year closely resemble last year's results (**figure 25**). Cross training of organizational personnel and increased use of contractors and consultants remain primary mitigations. Training increases two percentage points from last year, and increased use of contractors or consultants increases five percentage points, after a slight decrease in 2021. Artificial intelligence continues its upward trend to 25 percent, from 22 percent last year; however, its use in respondent security operations is unchanged from last year. Employer actions to overcome soft skill shortcomings are illustrated in **figure 26**.

FIGURE 25—MEANS OF MITIGATING TECHNICAL SKILLS GAPS

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

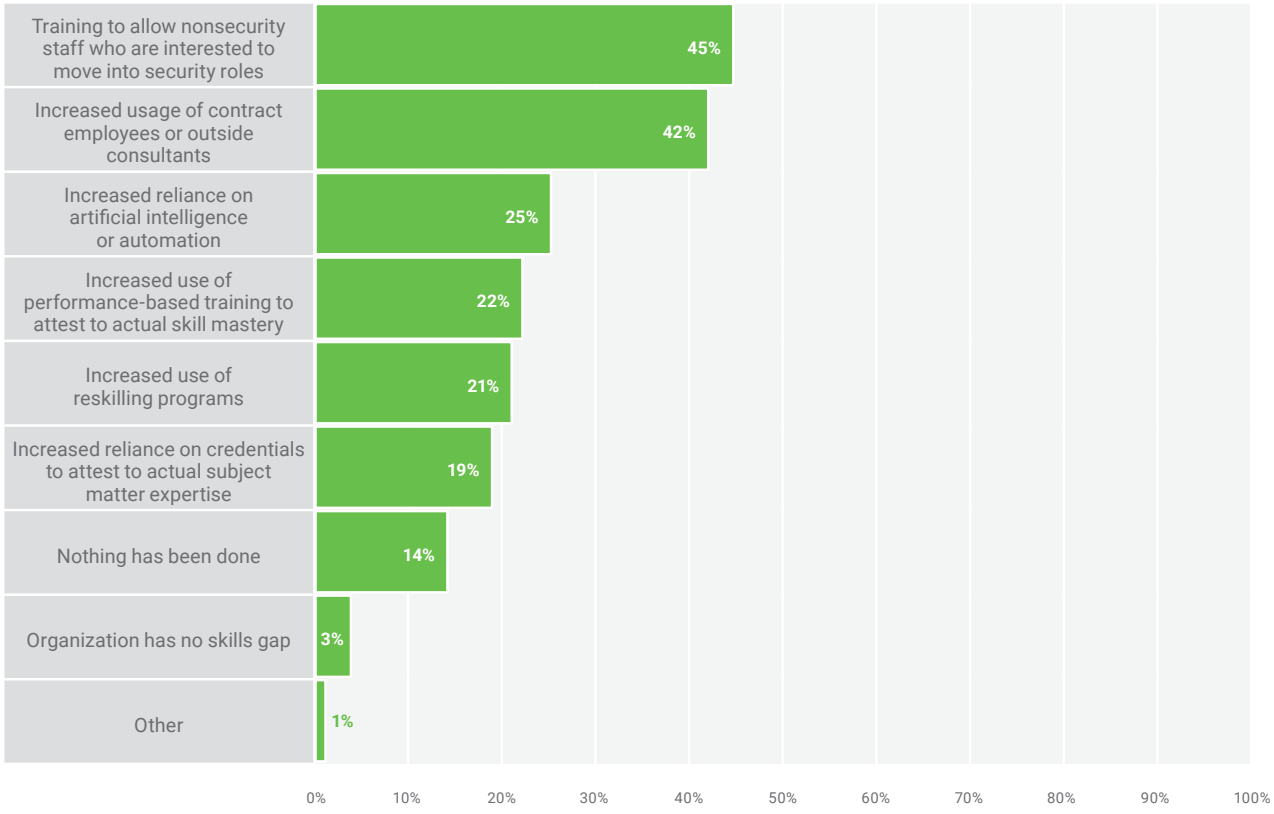
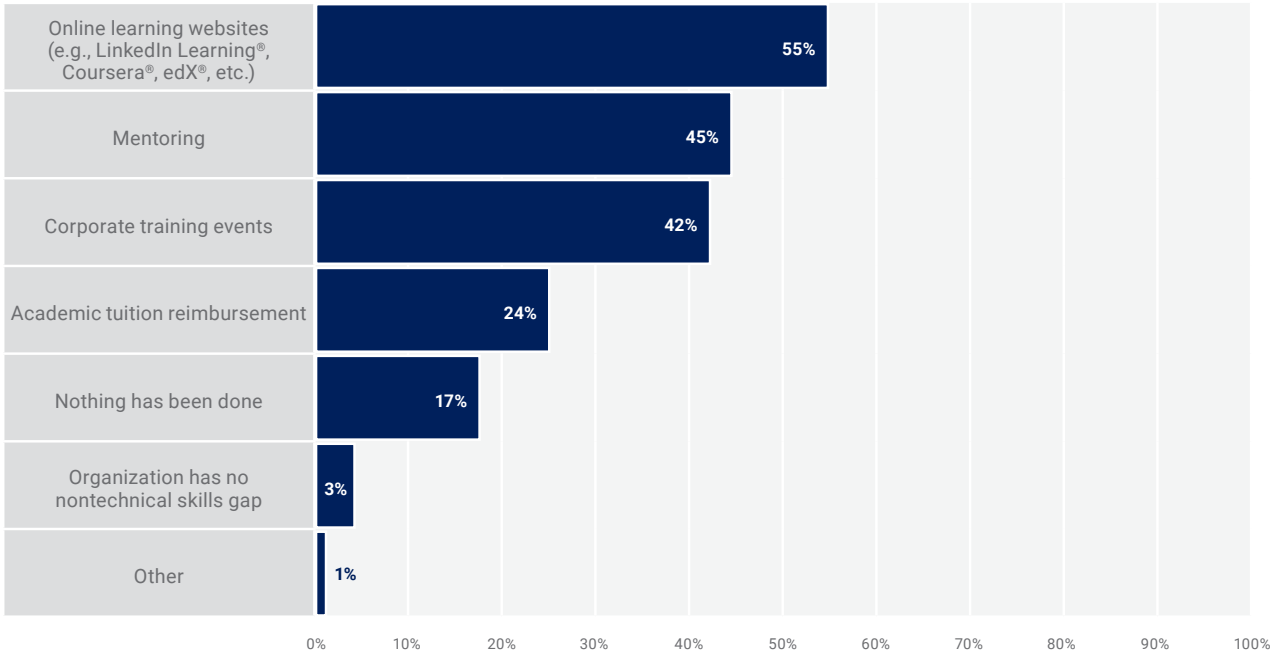


FIGURE 26—MEANS OF MITIGATING NONTECHNICAL SKILLS GAPS

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



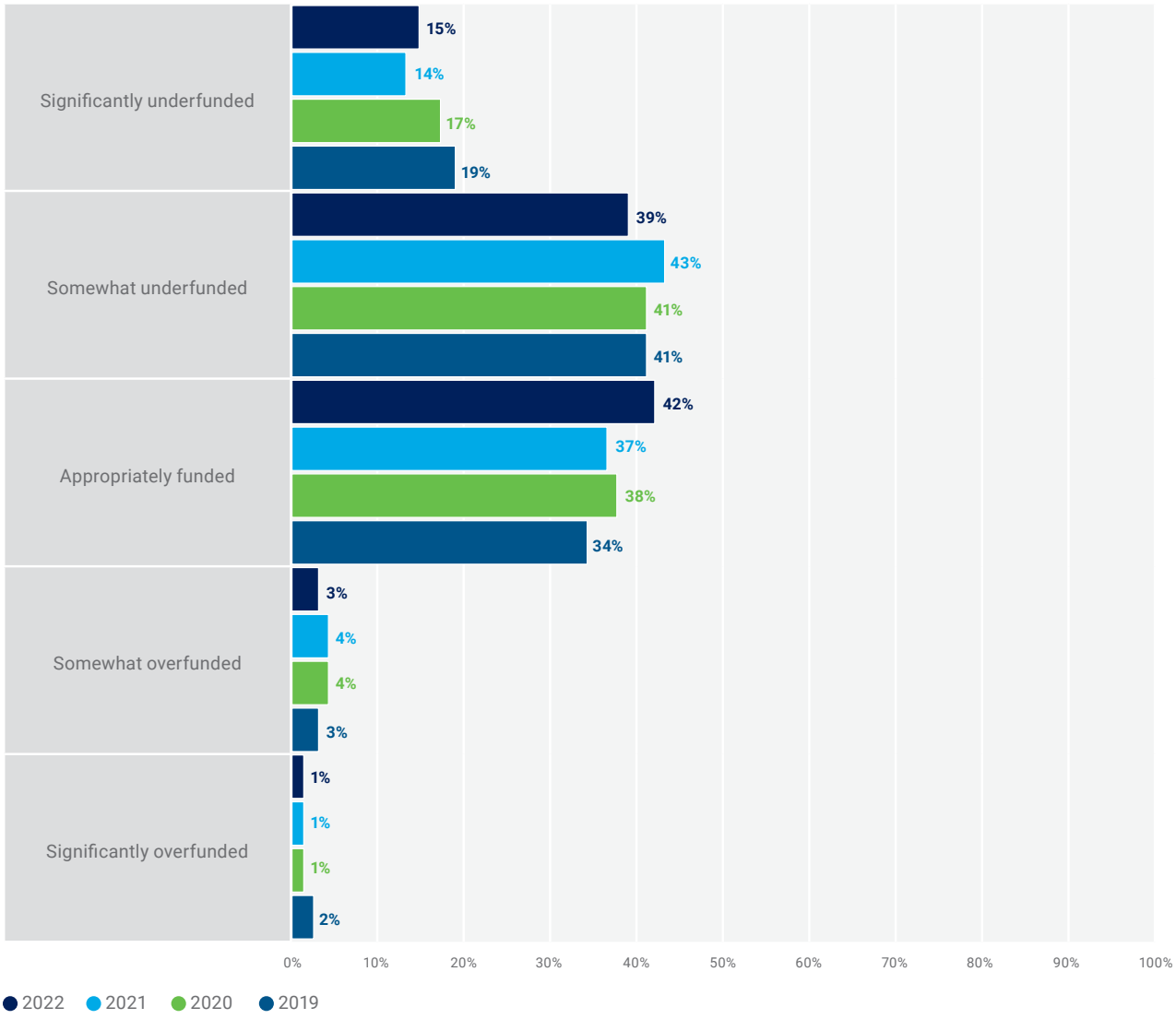
Cybersecurity Budgets Near Equilibrium

After three years of steady decreases in the number of survey respondents who believe their organization's cybersecurity budget is significantly underfunded (**figure 27**), this year's data suggest a slight course reversal, albeit by just one percentage point. What is clearly good news is that the number of survey respondents who believe their cybersecurity programs are appropriately funded is 42 percent—a five percentage-point increase and the most favorable report since ISACA began its state of cybersecurity reporting.

Survey respondents show overwhelming optimism about funding for next year, with 55 percent expecting budget increases (**figure 28**) while 38 percent expect no change. Multiyear data (**figure 29**) suggest that budgets are in fact leveling.

FIGURE 27—CYBERSECURITY FUNDING PERCEPTION

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



Survey respondents show overwhelming optimism about funding for next year, with 55 percent expecting budget increases, while 38 percent expect no change.

FIGURE 28—ENTERPRISE SECURITY BUDGET OUTLOOK

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

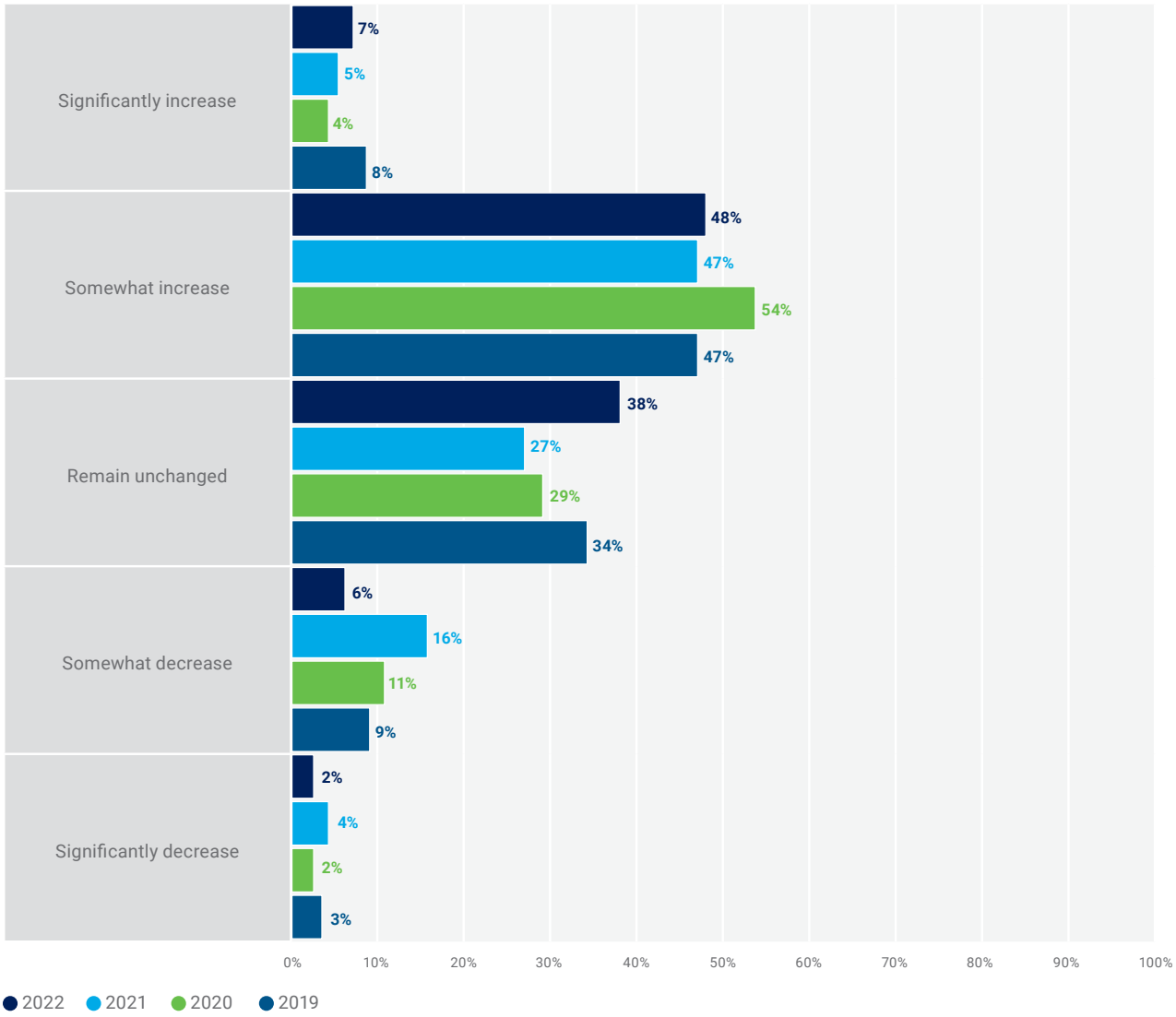
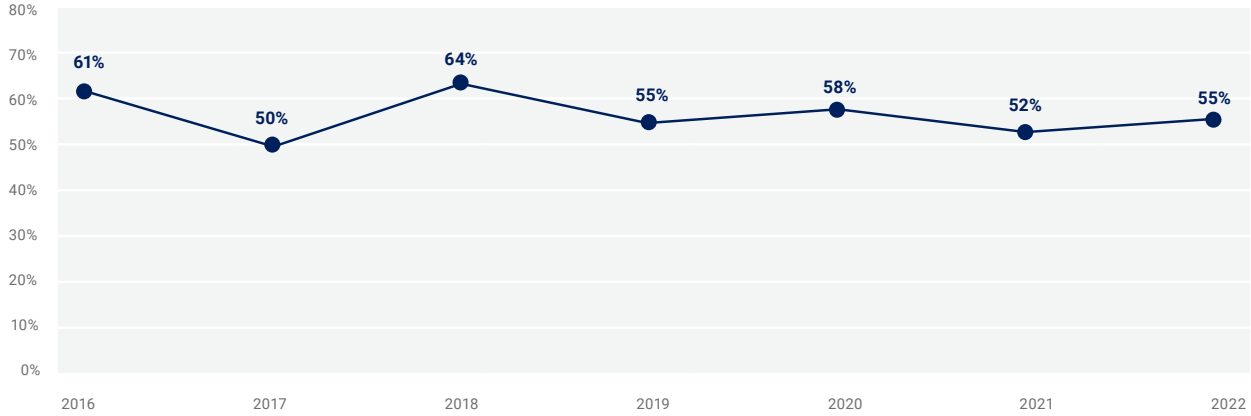


FIGURE 29—FORECASTED SECURITY BUDGET INCREASES (7 YEAR)



Threat Landscape

Despite a tumultuous year, the respondent data related to cybersecurity attack reporting in ISACA *State of Cybersecurity 2021, Part 2*,[12] more closely align with prepandemic data, as shown in the five-year comparison in **figure 30**. This year, 43 percent of respondents indicate that their organization is experiencing more cyberattacks (**figure 31**)—an eight percentage-point increase from last year. However, only 51 percent of respondents believe it is likely or very likely that their organization will experience a cyberattack in the coming year. This result seems overly optimistic, especially when considering that consumers believe cybercrimes increased in the past 12 months and nearly half of consumers in developed markets recognize they can be a victim of cybercrime, based on the ISACA *Consumer Cybersecurity Research Report*.[13] Nonetheless, approximately 20 percent of worldwide consumers (50 percent in India) believe there is zero likelihood of their becoming a victim of cybercrime,[14] ISACA's research suggests.

FIGURE 30—YEAR OVER YEAR COMPARISON OF CYBERSECURITY ATTACK REPORTING[15]

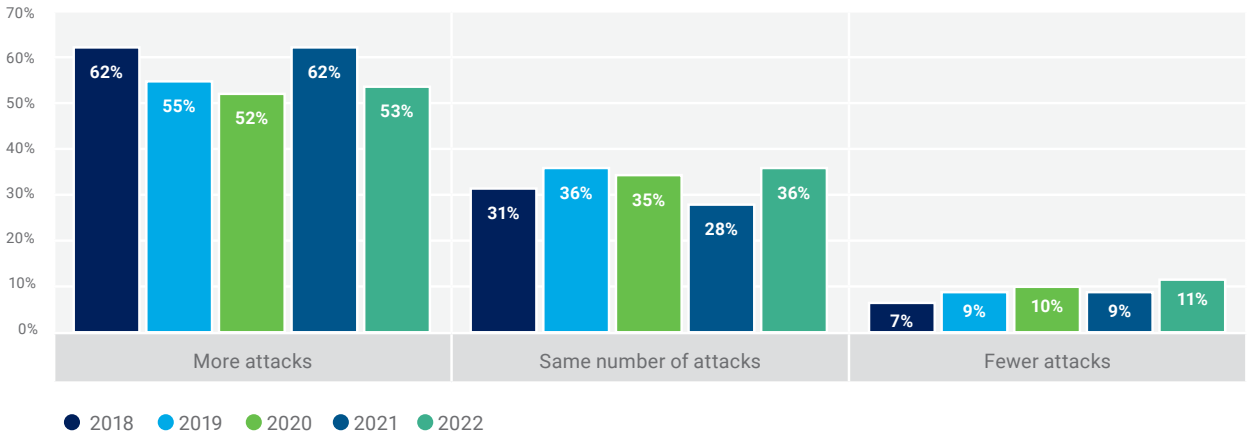
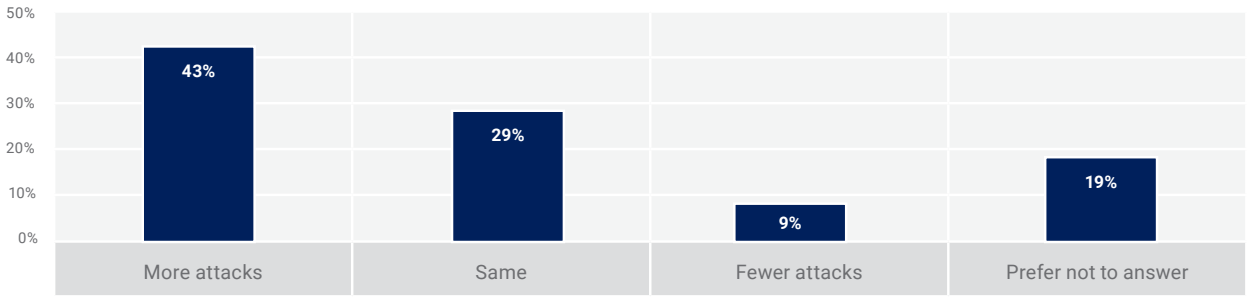


FIGURE 31—CHANGE IN NUMBER OF CYBERSECURITY ATTACKS

Is your enterprise experiencing an increase or decrease in cyberattacks as compared to a year ago?



12 ISACA, *State of Cybersecurity 2021, Part 2: Threat Landscape, Security Operations and Cybersecurity Maturity*, www.isaca.org/go/state-of-cybersecurity-2021

13 *Op cit* ISACA, *Consumer Cybersecurity Research Report*

14 *Ibid.*

15 The responses "I don't know" and "prefer not to say" are omitted from this figure.

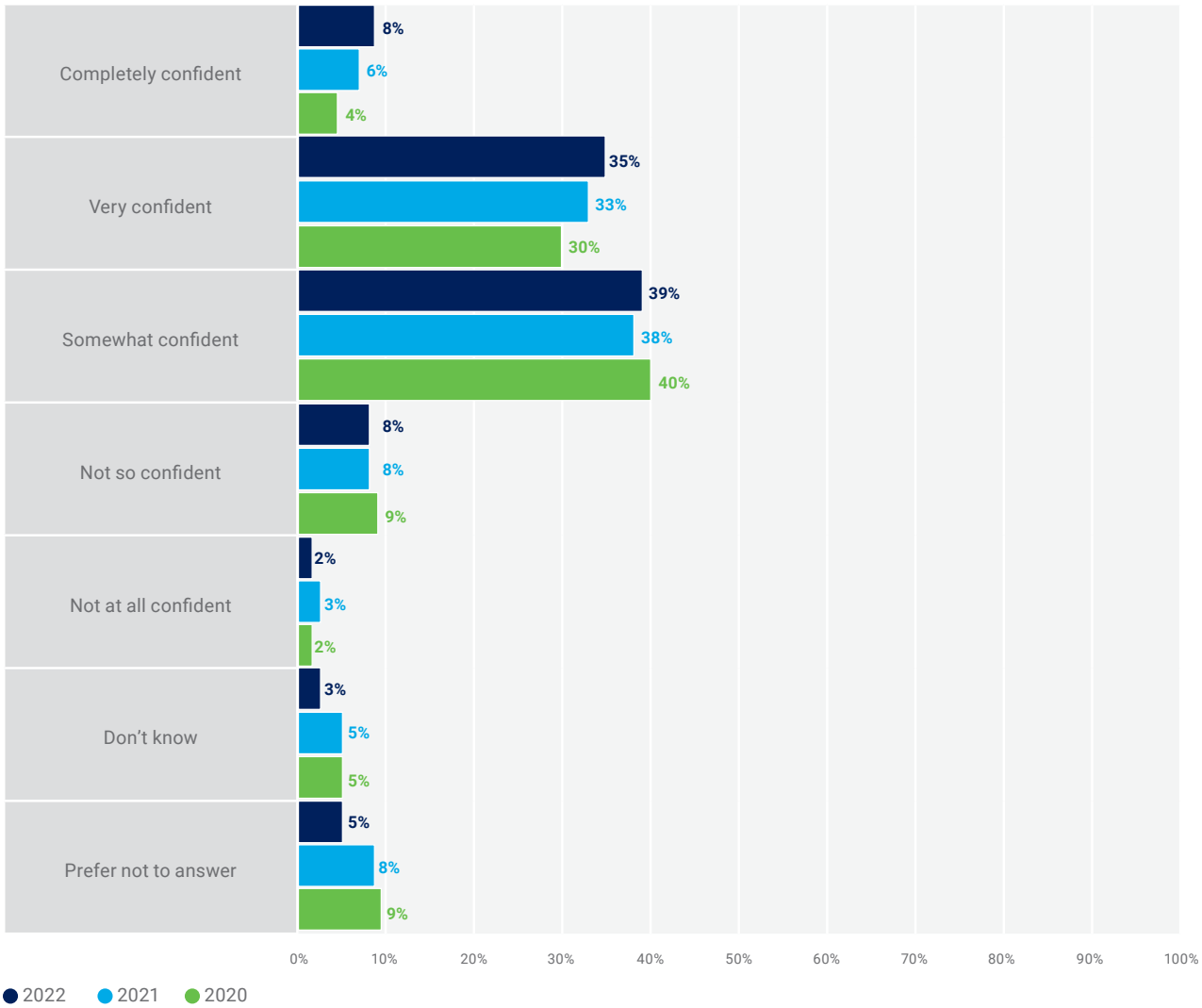
An Abundance of Confidence

Survey respondents' confidence in the ability of their cybersecurity team to detect and respond to cyberthreats reaches an all-time high of 82 percent[16]—a five percentage-point increase from last year (**figure 32**). This confidence is remarkable, considering that 46 percent of respondent enterprises have a security staff of just two to 10 individuals. Further, in-house staff fully manage approximately half of their five major security functions (identify, protect, detect, respond and recover), with most of the remainder partially outsourced.

Cybersecurity education and awareness training programs continue to positively impact overall employee awareness, with 80 percent[17] of survey respondents reporting at least some positive impact (**figure 33**).

FIGURE 32—ORGANIZATIONAL CONFIDENCE (2020-2022)

How confident are you overall in your organization's cybersecurity team's ability to detect and respond to cyberthreats?

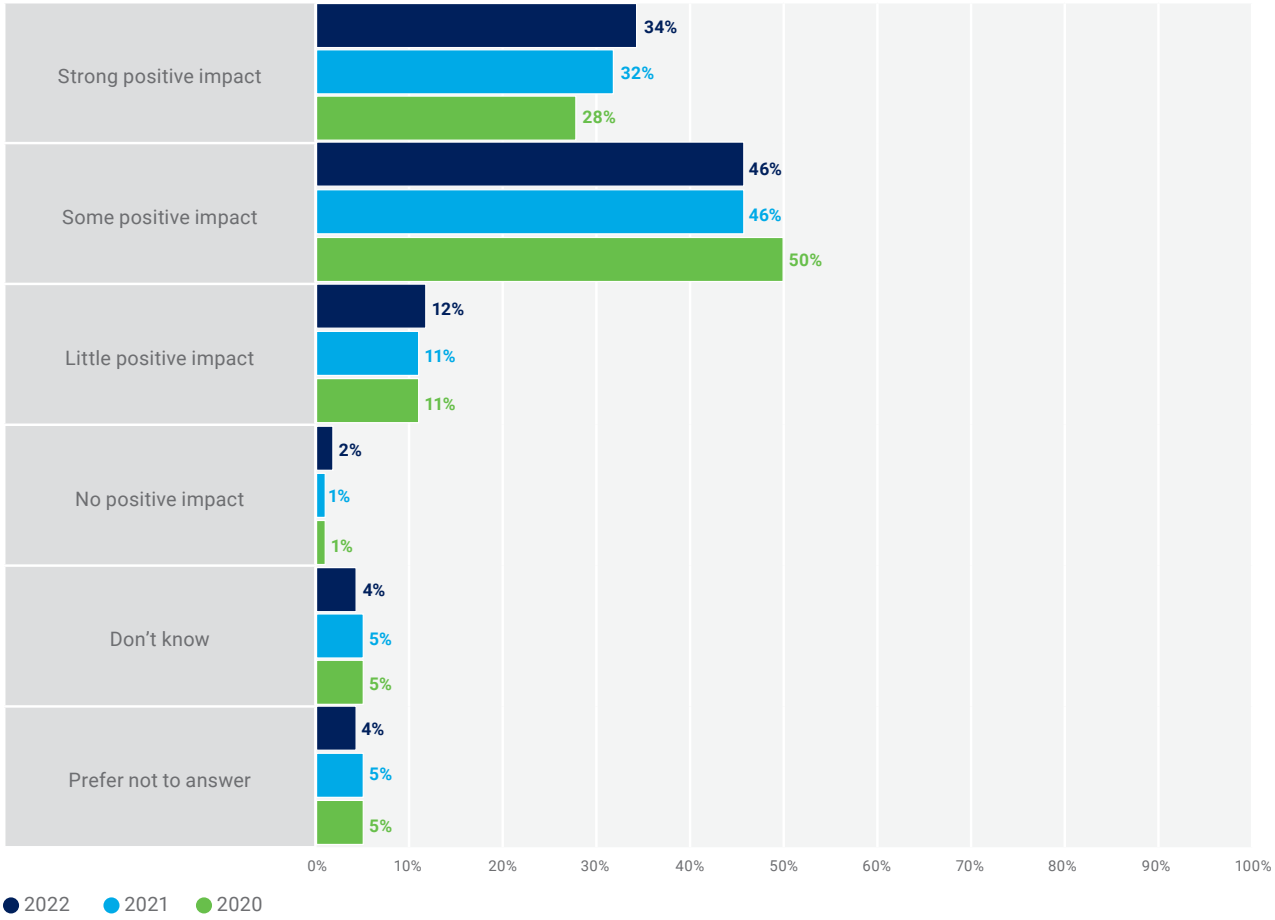


16 Eighty-two percent is the sum of completely confident responses (8%), very confident responses (35%) and somewhat confident responses (39%). It is the highest confidence response since ISACA introduced its *State of Cybersecurity* report eight years ago.

17 Eighty percent is the sum of the "strong positive impact" response (34%) and the "some positive impact" response (46%).

FIGURE 33—CYBERSECURITY AWARENESS PROGRAM IMPACT (2020-2022)

What impact, if any, do you feel that cybersecurity training and awareness programs have had on overall employee cybersecurity awareness in your organization?



Confidence in the ability of cybersecurity teams to detect and respond to cyberthreats reached an all-time high of 82 percent—a five percentage-point increase from last year.

Threat Actors and Attacks

The top three cyberattack concerns of survey respondents remain unchanged for the third consecutive year (**figure 34**):

- Enterprise reputation (79 percent)
- Data breach concerns (70 percent)
- Supply chain disruptions (54 percent)

Findings on sources of exploitation are also consistent with last year's results (**figure 35**). Twenty-five percent of respondents report that cybercriminals are responsible for their enterprise being exploited this year, 18 percent of exploits at respondent enterprises stem from hackers, and 11 percent of exploits at respondent enterprises are attributed to malicious insiders and nation-state actors. Of interest, nonmalicious insider exploits remain steady at 8 percent.

FIGURE 34—ORGANIZATIONAL CYBERSECURITY CONCERNS

What are your top concerns related to a cybersecurity attack on your organization? Select all that apply.

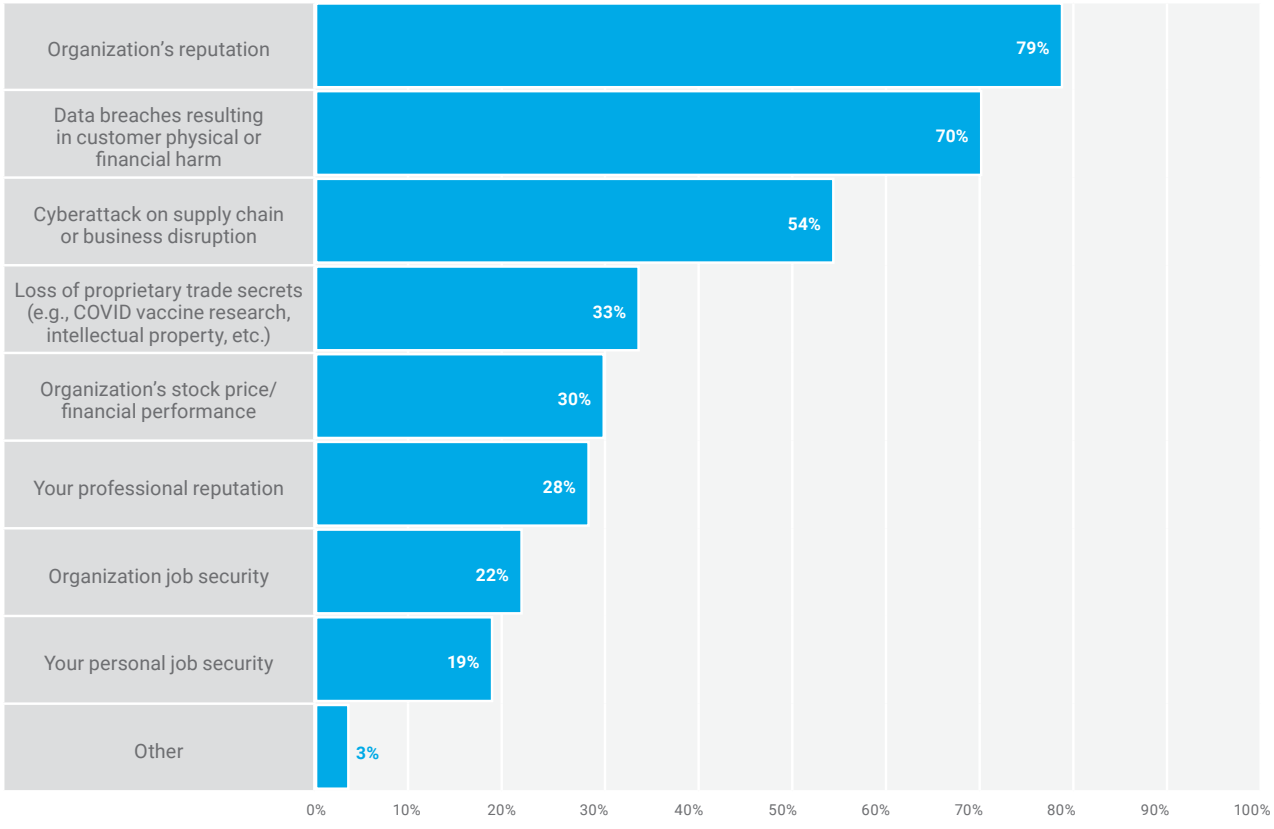
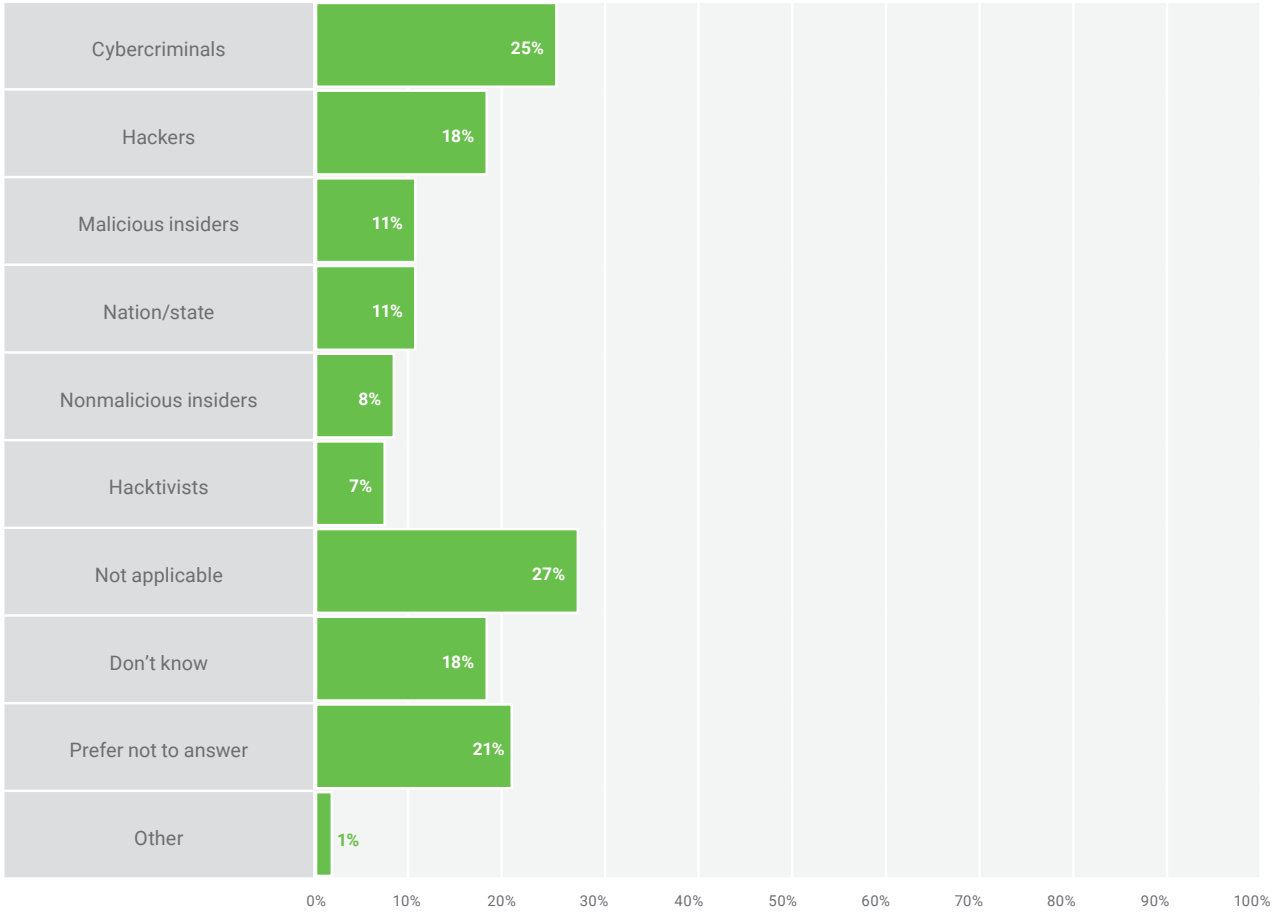


FIGURE 35—THREAT ACTORS

If your organization was exploited this year, which of the following threat actors were to blame? Select all that apply.



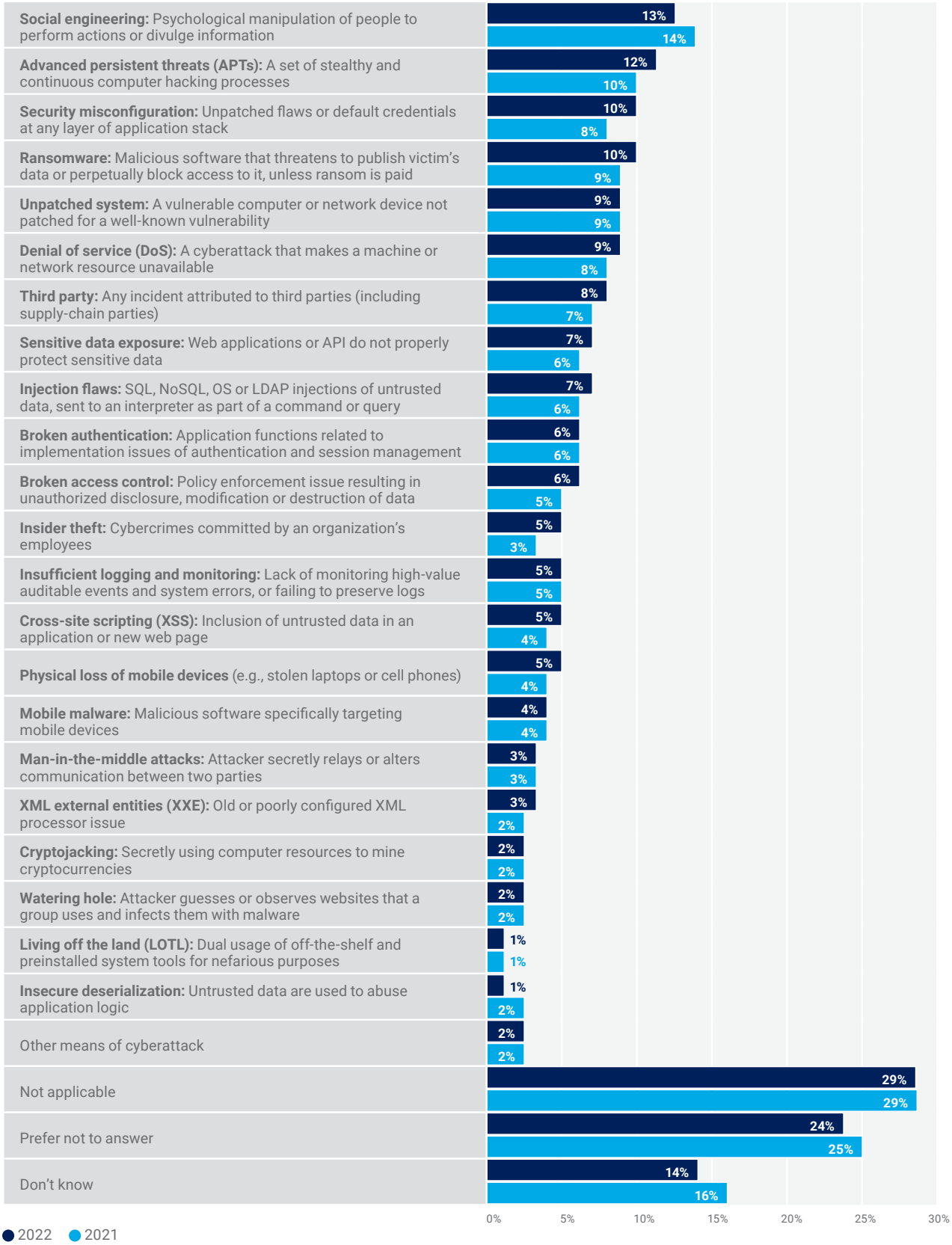
Social engineering remains the predominant cyberattack method (13 percent), followed by advanced persistent threat (APT) (12 percent), security misconfiguration (10 percent), ransomware (10 percent), unpatched system (9 percent) and denial of service (9 percent). Responses about attack types vary from the ISACA *State of Cybersecurity 2021, Part 2* report, as illustrated in **figure 36**. Despite high-profile attacks during this reporting period,[18] the percentage of respondents reporting ransomware attacks is only one point higher than a year ago, reinforcing the observation that high-profile press coverage does not necessarily reflect a change in the predominance of an attack type.

Despite high-profile attacks during this reporting period, the percentage of respondents reporting ransomware attacks is only one point higher than a year ago, reinforcing the observation that high-profile press coverage does not necessarily reflect a change in the predominance of an attack type.

18 Touro College Illinois, "The 10 Biggest Ransomware Attacks of 2021," 12 November 2021, https://illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php

FIGURE 36—ATTACK TYPES

If your organization was compromised this year, which of the following attack types were used? Select all that apply.



Cybersecurity Maturity—Barriers Limit Cyberrisk Assessment

ISACA introduced cybersecurity-maturity (cybermaturity) questions in the ISACA *State of Cybersecurity Survey* conducted at the end of 2020. Responses to these questions offer insight into the effectiveness of enterprise security investments and provide a baseline for comparative analysis this year and beyond. Fifty-five percent of respondents believe their board of directors adequately prioritizes enterprise cybersecurity and 75 percent believe that their enterprise cybersecurity strategy is aligned with enterprise objectives. These responses are largely in line with last year's survey data.

In this year's survey, 41 percent of respondents say their enterprises conduct cyberrisk assessments annually, compared with last year's 39 percent (**figure 37**). The two percentage-point increase is minor, and the annual interval—perhaps at best viewed as acceptable—likely is not frequent enough, given the rate at which enterprise digital ecosystems are changing.[19] The increase in the percentages of respondents whose enterprises perform cyberrisk assessments more often than annually is small (33 percent in 2022 and 32 percent in 2021), but it could signal a winning trend to watch.

Sixty-six percent of respondents' enterprises currently assess their cybermaturity—a near mirroring of 2021 data (**figure 38**).

Conducting cyberrisk assessments is critical to effective monitoring of risk factors and to improving response capabilities. Although the low percentage of enterprises that conduct cyberrisk assessments more often than annually appears to show a lack of prudence on this score, resource challenges and other constraints can limit some enterprises to making annual assessments.

Conducting cyberrisk assessments is critical to effective monitoring of risk factors and to improving response capabilities.

Enterprises face many obstacles to conducting frequent cyberrisk assessments. Time (cited by 43 percent of respondents) was the primary barrier, followed by lack of personnel to perform assessments (40 percent). See **figure 39** for all responses.

19 Tech-Wonders.com, "How Often Should Your Business Perform Cyber Risk Assessment," www.tech-wonders.com/2021/10/how-often-should-your-business-perform-cyber-risk-assessment.html

FIGURE 37—CYBERRISK ASSESSMENT (2021-2022)

How often is a cyberrisk assessment performed on your organization?

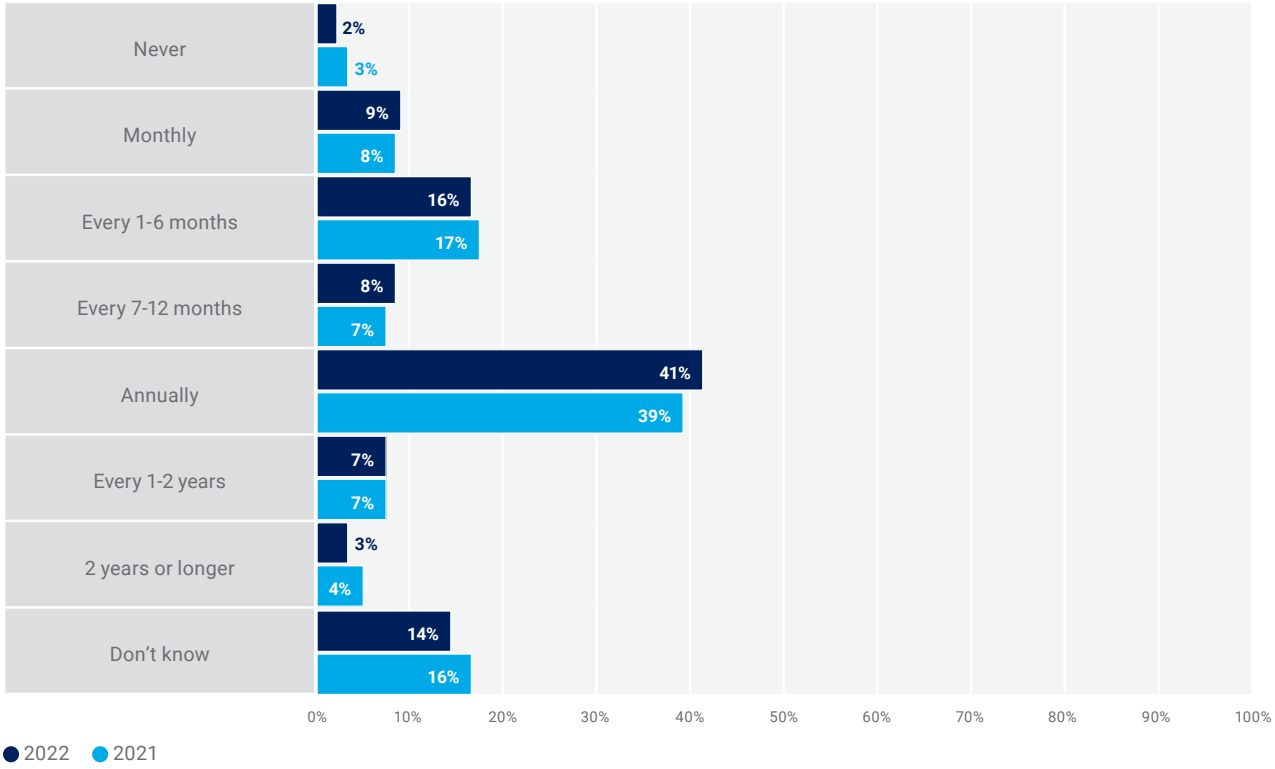


FIGURE 38—CYBERMATURITY ASSESSMENT

Does your organization currently assess its cybermaturity?

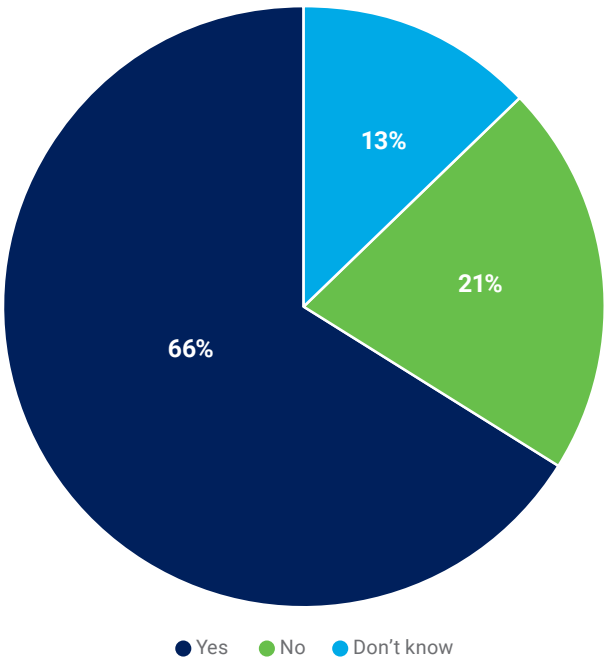
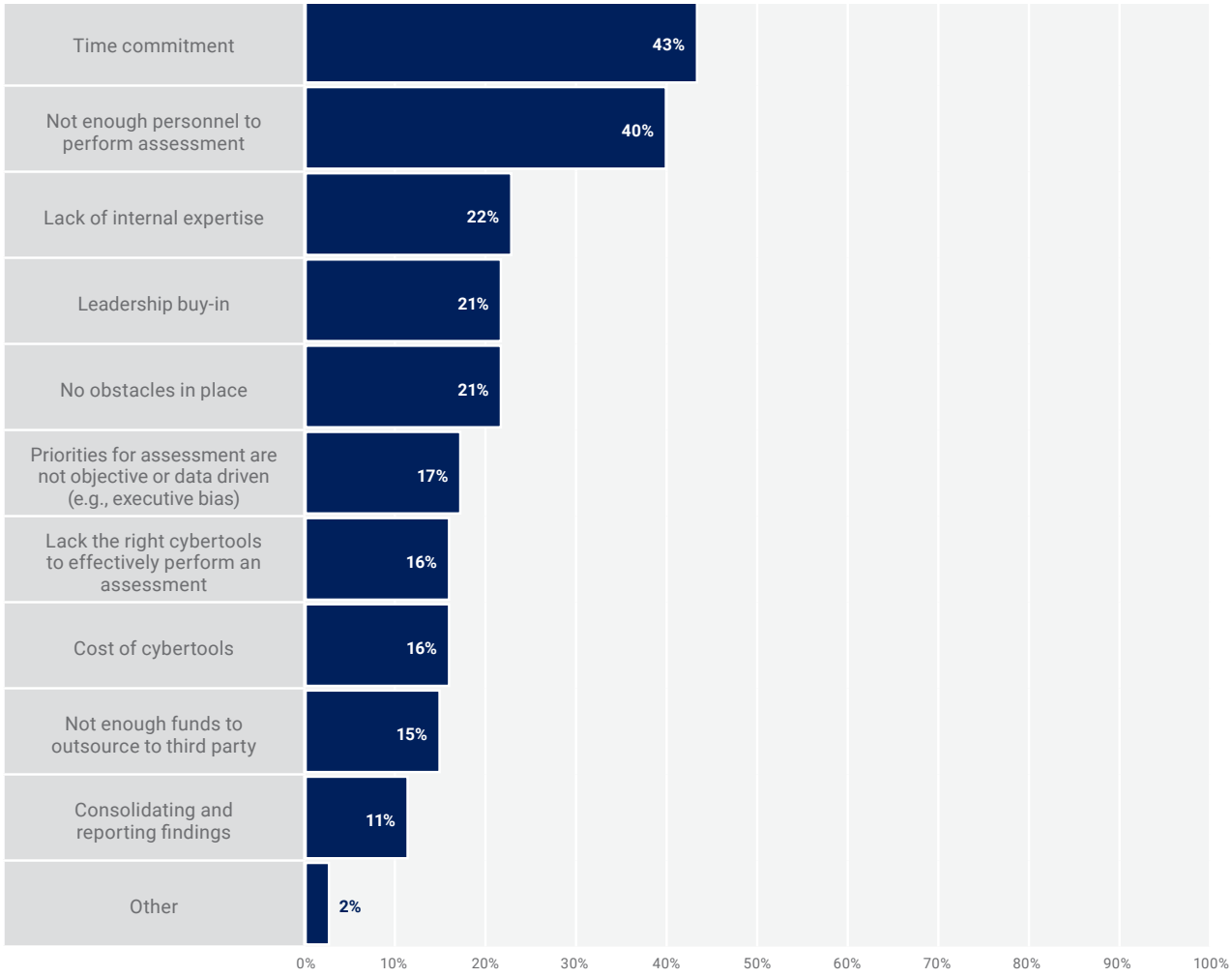


FIGURE 39—CYBERRISK ASSESSMENT OBSTACLES

Which, if any, obstacles does your organization face in conducting a cyberrisk assessment? Select all that apply.



Conclusion—Big News Is Not Always Big Data

The cybersecurity workforce shortage is not going away. It appears to be getting worse, perhaps influenced by job seekers considering flexible working hours a major factor in stay-or-go decisions. Enterprises that support or favor remote work have an advantage attracting qualified talent.[20] Resilience is key—especially in today's high-demand, low-supply industries. A lengthy time to fill vacancies increases workplace stress and can influence employees to look elsewhere for opportunities that more closely match their desired work-life balance.

Formal education programs offer benefits; however, respondent data affirm that employers are heeding the advice of ISACA and many others by removing degree requirements—especially for entry-level positions. At a minimum, recategorizing degrees as desirable versus required increases the potential talent pool for an enterprise.

Given the ongoing seller's market for cybersecurity professionals, enterprises are encouraged to focus on competitive total benefits packages as opposed to competitive salaries alone. Salary expectations vary, but it is likely that many small- to medium-size enterprises simply cannot compete with larger enterprises on salary. With the likelihood that budgets will continue to level, enterprises may find themselves constrained with respect to additional headcount salaries and should therefore identify other ways to remain competitive in sourcing and retaining talent.

Cyberattack reporting is mostly unchanged from last year and, despite the media buzz surrounding ransomware attacks during this reporting cycle, the data nearly mirror the results of a year ago.

Cybermaturity efforts take time and human capital—both of which are in short supply within the industry. Finally, although nearly half the surveyed enterprises have settled into a yearly risk assessment cycle, that interval is not optimal. It allows too much time for significant environmental deviations to occur, which could weaken response plans and undermine organizational resilience.

20 Kier, L.; "Remote Work: The Ultimate Equalizer for Talent Acquisition and Employee Experience," *Forbes*, 10 August 2020, www.forbes.com/sites/forbescommunicationscouncil/2020/08/10/remote-work-the-ultimate-equalizer-for-talent-acquisition-and-employee-experience/?sh=714d56d57986

Acknowledgments

ISACA would like to recognize:

Board of Directors

Gregory Touhill, Chair
CISM, CISSP
Director, CERT Division of Carnegie Mellon University's Software Engineering Institute, USA

Pamela Nigro, Vice-Chair
CISA, CGEIT, CRISC, CDPSE, CRMA
Vice President, Security, Medecision, USA

John De Santis
Former Chairman and Chief Executive Officer, HyTrust, Inc., USA

Niel Harper
CISA, CRISC, CDPSE, CISSP
Former Chief Information Security Officer and Privacy Officer, United Nations Office for Project Services (UNOPS), Denmark

Gabriela Hernandez-Cardoso
Independent Board Member, Mexico

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

Veronica Rose
CISA, CDPSE
Founder, Encrypt Africa, Kenya

David Samuelson
Chief Executive Officer, ISACA, USA

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

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

Tracey Dedrick
ISACA Board Chair, 2020-2021
Former Chief Risk Officer, Hudson City Bancorp, USA

Brennan P. Baybeck
CISA, CISM, CRISC, 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

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 LookingGlass

LookingGlass develops cybersecurity solutions that empower organizations to meet their missions and reduce cyberrisk with a comprehensive view of their attack surface—outside-in and inside-out—layered with actionable threat intelligence. By linking the risk and vulnerabilities from an organization's attack surface to customized threat actor models, LookingGlass provides a more accurate view of cyberrisk and enables systematic definition and deployment of mitigations to defend against the threats that matter.

Learn more at https://lookingglasscyber.com.

Disclaimer

ISACA has designed and created *State of Cybersecurity 2022: Global Update on Workforce Efforts, Resources and Cyberoperations* (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.

State of Cybersecurity 2022: Global Update on Workforce Efforts, Resources and Cyberoperations

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

Learn more:
www.isaca.org/state-of-cybersecurity-2022

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/

LOOKINGGLASS

"LookingGlass provides the data, in whatever format we need, that helps **pinpoint** and **prioritize** what and where we need to be looking to **jumpstart** our investigations. Without LookingGlass, some of our most effective operations would slow to a crawl or stop."

– U.S. Federal Law Enforcement Agency

"LookingGlass is **essential** to our third-party risk management program. Their non-invasive, **continuous** monitoring capability complements our organization's point-in-time, questionnaire-based assessment process, giving us a **holistic** view of our suppliers' overall information and cybersecurity posture."

– Fortune 100 Financial Services Company

Get the Intelligent View of Your Attack Surface.
Find out more at LookingGlassCyber.com.