ISACA Adobe

State of Cybersecurity 2023

Global Update on Workforce Efforts, Resources and Cyberoperations

Information Security

CONTENTS

ABSTRACT

State of Cybersecurity 2023, Global Update on Workforce Efforts, Resources and Cyberoperations reports the results of the annual ISACA® global State of Cybersecurity Survey, conducted in the second quarter of 2023. This survey report focuses on the current trends in cybersecurity workforce development, staffing, cybersecurity budgets, threat landscape and cybermaturity. At a high level, the 2023 survey data largely bolstered and even appeared to mirror last year's data. However, further analysis revealed some subtle shifts, possibly influenced by geopolitical, economic and technological advances.

Executive Summary

The ninth annual ISACA® global *State of Cybersecurity Survey* continues to identify current challenges and trends in the cybersecurity field. For the second consecutive year, ISACA fielded questions to gain deeper insight into persistent issues in cybersecurity workforce skill sets and staffing for entry-level positions. *The State of Cybersecurity 2023* report analyzes the survey results on cybersecurity skills and staffing, resources, cyberthreats and cybersecurity maturity.

The survey findings are largely consistent with the findings from previous years, with any shifts likely linked to economic uncertainty, technological advances and the timing of well-known cybersecurity incidents. Uncertainty of any kind appears to be driving fewer job changes, and while vacancies persist, the survey results indicate that enterprises appear to be tightening budgets and compensation aids ahead of a potential recession.

Key findings of the survey include the following:

- The percentage of respondents who manage security staff with less than three years of work experience remains unchanged from prior years, while demographic information among respondents indicates an aging workforce.
- Seventy-one percent of survey respondents have unfilled cybersecurity positions, with unfilled non-entry-level positions outnumbering entry-level positions by twofold. Those stating that their organization had no open positions grew by six percentage points.
- Employer benefits are tightening with notable declines in tuition reimbursement and recruitment bonuses. Paid volunteer time off increased.
- Soft skills remain the largest skill gap among cybersecurity professionals and university graduates, though views on the former have worsened. Among current practitioners, cloud computing skills improved by five percentage points from 2022. Technical skills among university graduates largely resembled 2022 data, with slight improvements in security controls and network operations; of concern with this group is the four-percentage-point drop in networking-related competency.
- Cross-training of employees and increased use of contractors and consultants remain primary mitigation approaches to address the workforce shortage.
- While the percentage of employers requiring a university degree for entry-level cybersecurity positions remains at 52 percent, differences across geographical regions are notable—Europe and Africa saw decreases, Asia and North America remained unchanged, and Latin America and Oceania reported large increases in this requirement.

Respondents' views on the appropriateness of cybersecurity program funding are statistically the same as in 2022. Last year's optimism surrounding cybersecurity budgets was short-lived; now, the prominent view is that the next budget cycle will result in the expectation of doing more with less. Annual cyberrisk assessments continue, with data pointing to smaller improvements being made more frequently.

Last year's optimism surrounding cybersecurity budgets was short-lived; now, the prominent view is that the next budget cycle will result in the expectation of doing more with less.

While the alignment of the security leader and cybersecurity team has no bearing on the cadence of enterprise cyberattacks, enterprises that prioritize cybersecurity at the board of directors' level and align their cybersecurity strategy with their organizational objectives are more likely to have a Chief Information Security Officer (CISO) and a cybersecurity team that reports to the CISO. Enterprises lacking this alignment are more likely to have the cybersecurity team report to the Chief Information Officer (CIO) and twice as likely not to have a CISO or Chief Security Officer (CSO).

Survey Methodology

In the second quarter of 2023, 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 job titles in the information security field. Of those invited, a total of 2,178 respondents completed the survey in its entirety, and their responses are included in the results.[1] The survey data were collected anonymously. This survey has a margin of error of +/- 2 percent at a 95 percent confidence interval.

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's target population includes individuals who have cybersecurity job responsibilities. Of the 2,178 respondents, 53 percent indicate that cybersecurity is their primary professional area of responsibility. **Figure 1** shows demographic information about the respondents, who hail from 112 countries and territories. **Figure 2** further illustrates the breadth of survey input, showing that respondents represent more than 17 industries.

Cybersecurity Workforce Challenges Here to Stay

General workforce estimates in the industry appear to indicate that the cybersecurity job market offers a tremendous opportunity for all aspiring cybersecurity practitioners and career changers. To date, the multibillion-dollar global cybersecurity training market,[2] abundance of university programs and countless other initiatives (e.g., apprenticeships, reskilling, scholarships) have been unable to reverse the supply-demand imbalance. However, despite the growing estimates of the lack of supply to meet demand, there is little evidence of meaningful progress. Continued hyper-focus on the perceived worker shortage to fill unverifiable open cybersecurity positions is problematic, for it not only fails to address duplicate job postings but also the perspectives of aspiring cybersecurity professionals who spent significant time and money completing pathway programs and yet remain unable to secure employment in the cybersecurity field. While the United States National Cyber Workforce and Education Strategy (NCWES)[3] and similar efforts globally may be comprehensive, they cannot compel enterprises to create entry-level positions. Failure to resolve this critical issue will magnify the existing problem of students and career changers being unable to obtain employment due to lack of experience, despite any knowledge, skills or credentials they have acquired.

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.

2 Patil, V.; "Cyber Security Training Market Report 2022 – Research with Future Trends," LinkedIn, 20 January 2023, https://www.linkedin.com/pulse/cyber-security-training-market-report-2022-research-vinayak-patil/

3 The White House, "National Cyber Workforce and Education Strategy: Unleashing America's Cyber Talent," 31 July 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/31/fact-sheet-biden

FIGURE 1: Respondent Demographics

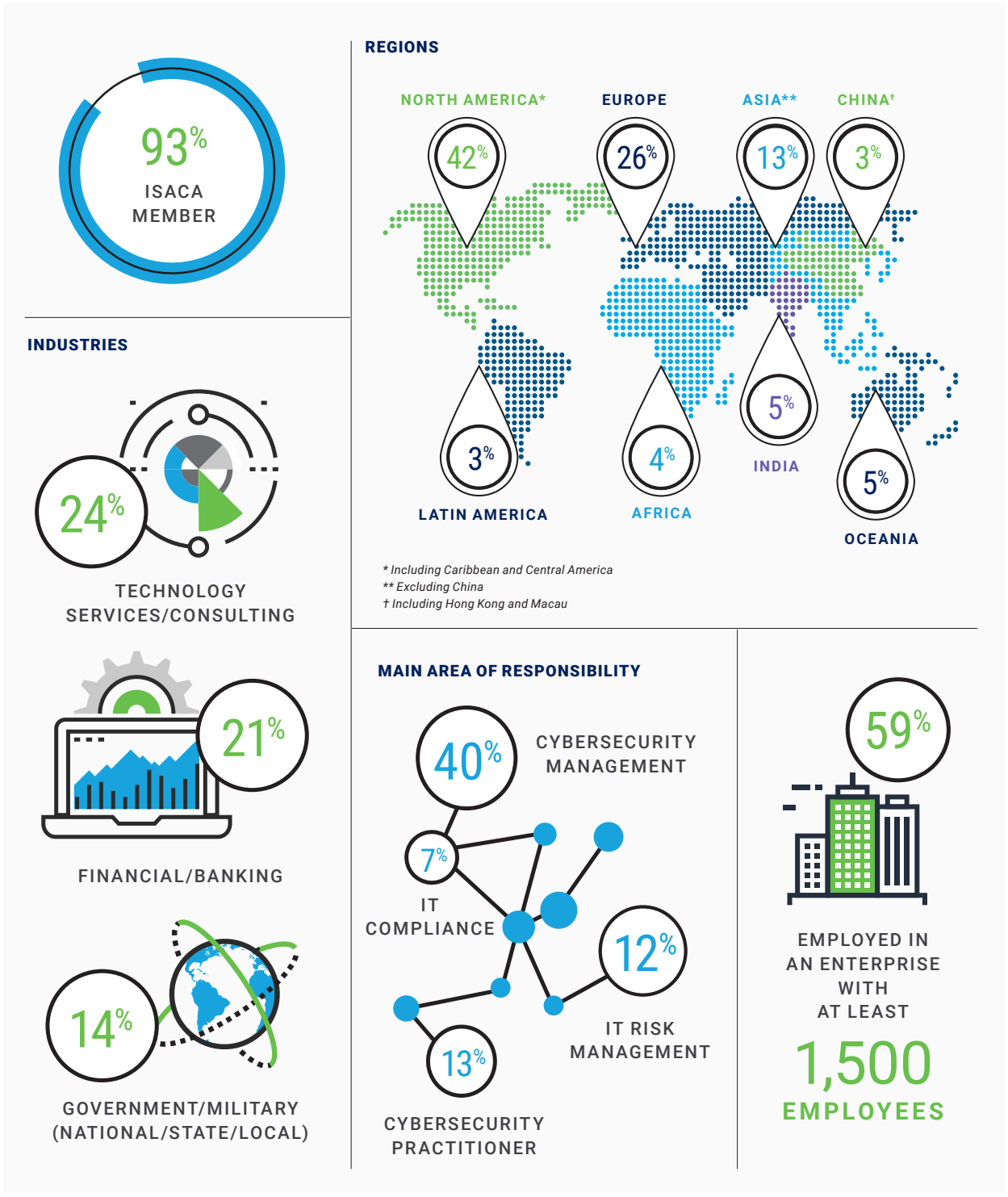
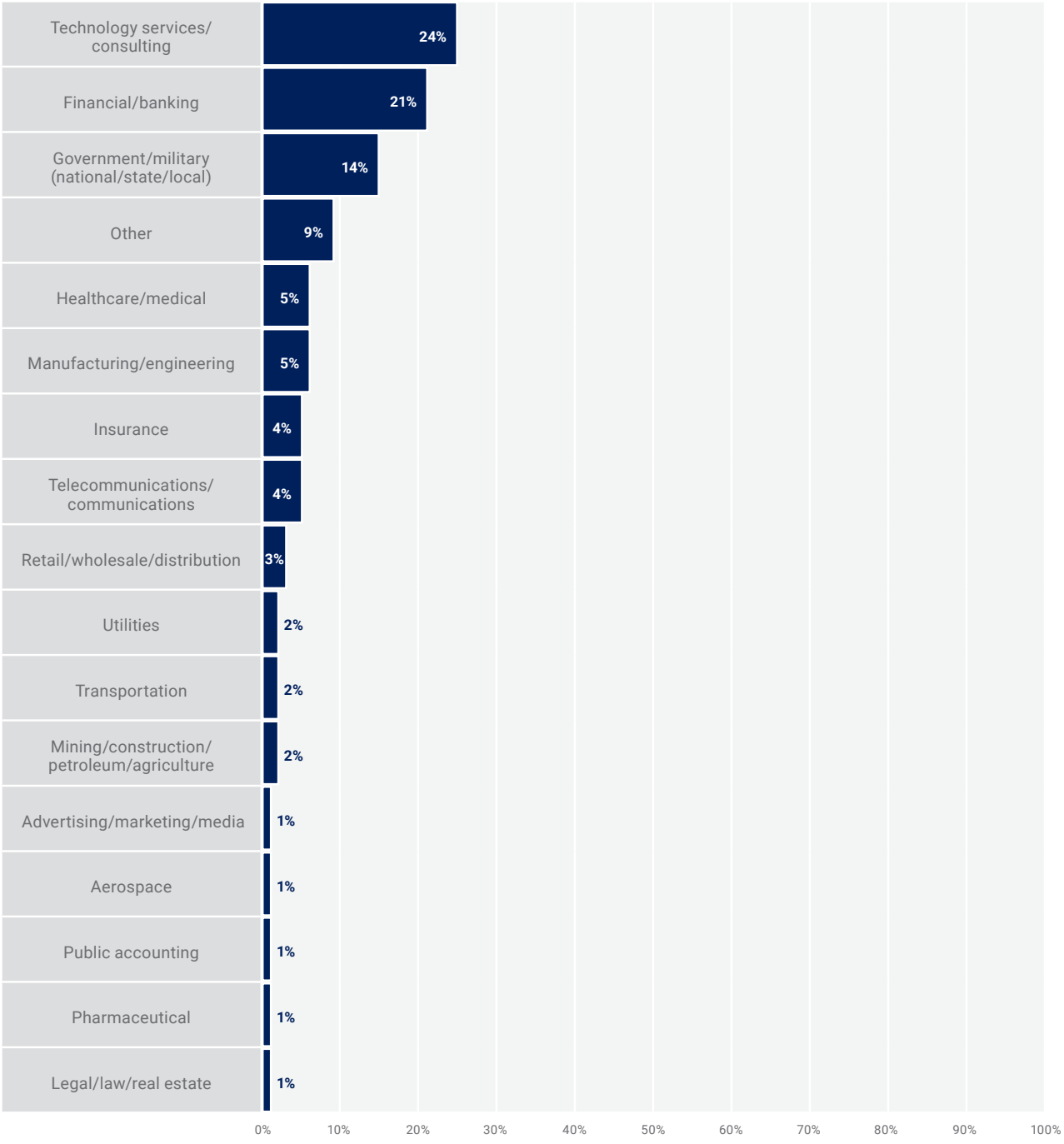


FIGURE 2: Industries Represented

Please indicate your organization's primary industry.



The current state of cybersecurity could not paint a more dire picture—an aging workforce coupled with too few entry-level positions. The existence of gatekeeping[4, 5] and problematic job descriptions[6] worsens the situation and amounts to self-inflicted pain points that no number of reskilling programs will help overcome. And yet, an already fragile situation has been made worse by employee burnout,[7] economic uncertainty[8] and a surge in return-to-office mandates.[9, 10] With economists forecasting a potential recession with varying degrees of certainty,[11] the movement that drove record employee job changes—the Great Resignation—is likely behind us, and uncertainty is forcing employees to stay put.[12] Current economic variations may not be enough to disrupt the seller's market enjoyed by experienced cybersecurity professionals, but there is evidence to support the belief that businesses are tightening the proverbial purse strings by way of benefits cuts.

The current state of cybersecurity could not paint a more dire picture—an aging workforce coupled with too few entry-level positions.

Staffing

The percentage of ISACA survey respondents who manage security staff with less than three years of work experience is unchanged at 44 percent. Workforce pipeline challenges continue to strain an increasingly aging workforce. While the largest percentage of respondents (34 percent) are between ages 35 and 44, the number of respondents older than 44 years of age increased, with respondents in the 45 to 54 and 55 to 64 age ranges increasing two percentage points (32 percent) and three percentage points (19 percent), respectively, from 2022 (**figure 3**).

This year's survey findings on staffing largely resemble the trends observed last year (**figure 4**). Regardless of age, respondents overwhelmingly felt the speed of filling open cybersecurity positions within their organization was unchanged this year (40 percent), while 20 percent believe it somewhat increased.

Retention challenges decreased this year, but the picture is not rosy. Over half (56 percent) of respondents indicated their organization struggles to retain talent, compared to 60 percent last year. And while employee burnout within the career field is well known,[13] economic uncertainty may be a contributing factor causing fewer career moves and marginal improvement in retention. Multiyear data suggest that uncertainty of any type influences employees to remain in place (**figure 5**).

4 Markel, D.; "Gatekeeping Has No Place In Cybersecurity," *Forbes*, 7 October 2022, https://www.forbes.com/sites/forbestechcouncil/2022/10/07/gatekeeping-has-no-place-in-cybersecurity/?sh=b60f4b35fdd4

5 SC Magazine, "Gatekeeping in Cybersecurity, Part 1 – Naomi Buckwalter–SCW #83," 17 August 2021, https://www.scmagazine.com/podcast-segment/gatekeeping-in-cybersecurity-part-1-naomi-buckwalter-scw-83

6 Pratt, K.M.; "6 security analyst job description red flags that make hiring harder," CSO, 18 July 2022, https://www.csoonline.com/article/573115/6-security-analyst-job-description-red-flags-that-make-hiring-harder.html

7 Townsend, K.; "Burnout in Cybersecurity–Can It Be Prevented?," Security Week, 22 March 2023, https://www.securityweek.com/burnout-in-cybersecurity-can-it-be-prevented/

8 Markovitz, G.; S. Feingold (eds.); "Recession in 2023? That depends on where you are in the world," World Economic Forum, 16 January 2023, https://www.weforum.org/agenda/2023/01/global-recession-economic-outlook-2023/

9 Lebowitz, S.; M. Ward; E. Canal; R. Knight; A. York; "Here's a list of major companies requiring employees to return to the office," Business Insider, 19 July 2023, https://www.businessinsider.com/companies-making-workers-employees-return-to-office-rto-wfh-hybrid-2023-1

10 Peck, E.; "Companies get aggressive on return-to-office," Axios.com, 13 June 2023, https://www.axios.com/2023/06/13/companies-aggressive-return-to-office

11 Saul, D.; "Will The U.S. Enter The Recession Experts Warned About For Months? It's Complicated," Forbes, 16 August 2023, https://www.forbes.com/sites/dereksaul/2023/08/16/will-the-us-enter-the-recession-experts-warned-about-for-months-its-complicated

12 Casselman, B.; "The 'Great Resignation' Is Over. Can Workers' Power Endure?," *The New York Times*, 6 July 2023, https://www.nytimes.com/2023/07/06/business/economy/jobs-great-resignation.html

13 Budge, J.; J. Roberts; H. Shey; D. Levine; "We Need To Talk More About Burnout In Cybersecurity," Forrester.com, 14 February 2023, https://www.forrester.com/blogs/we-need-to-talk-more-about-burnout-in-cybersecurity/

FIGURE 3: Workforce by Age

Please select your age.

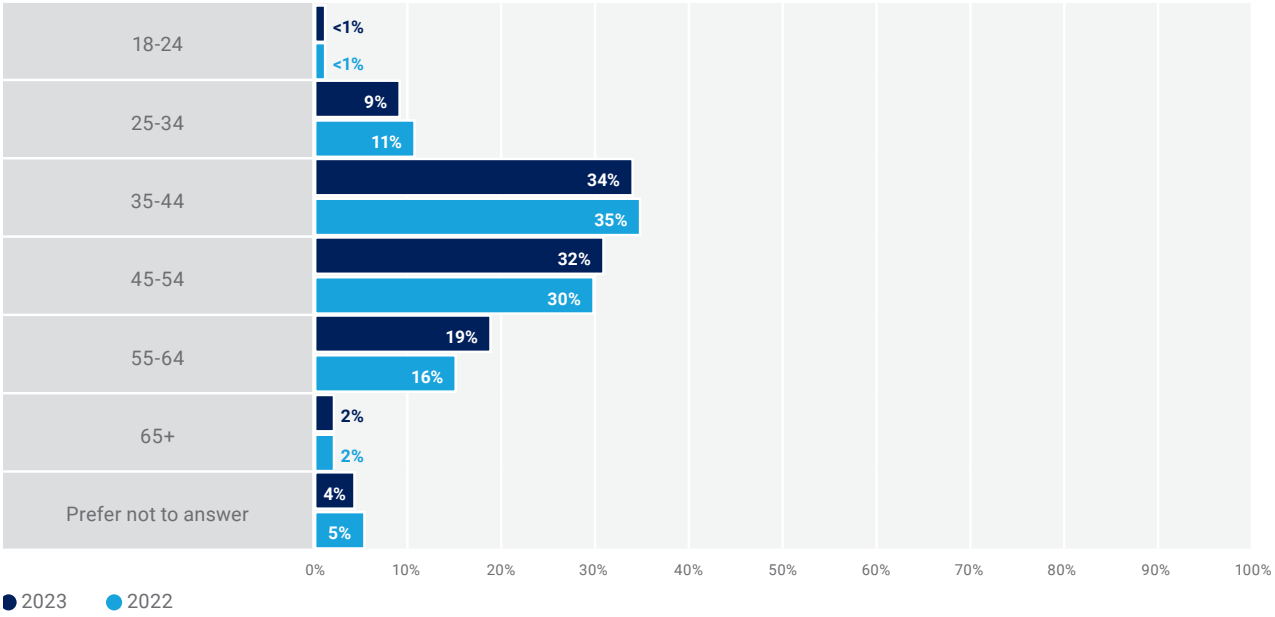


FIGURE 4: Cybersecurity Staffing

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

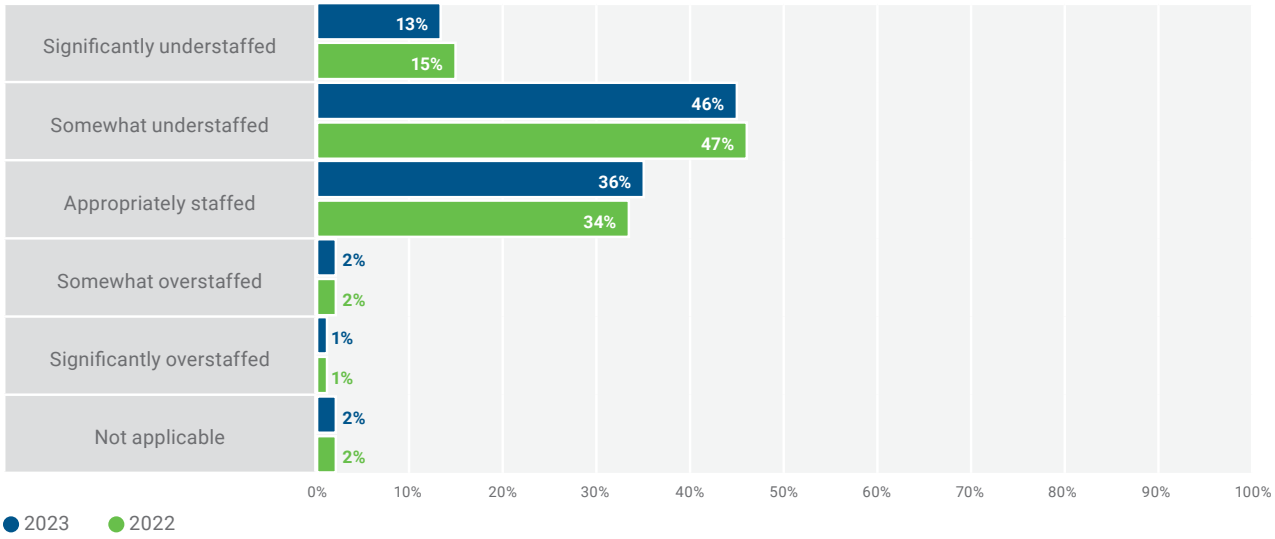
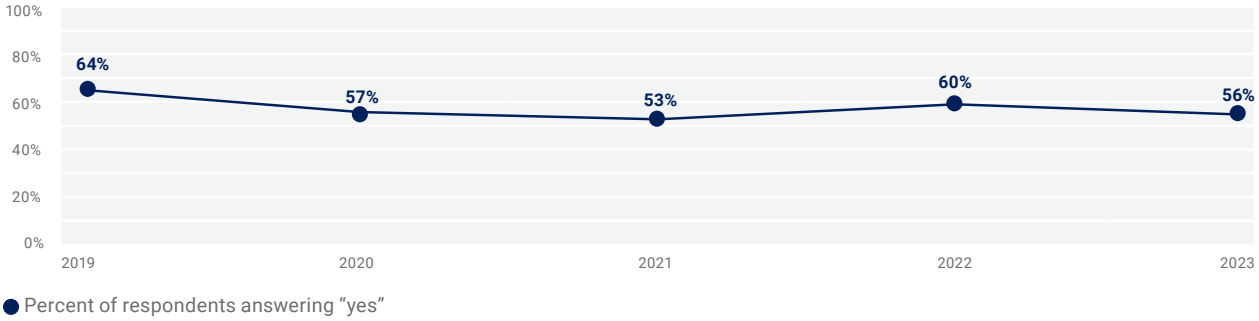


FIGURE 5: Retention Difficulties (2019-2023)

Has your organization experienced difficulties retaining qualified cybersecurity professionals?



Vacancies

Survey data (**figure 6**) offer good news for hiring managers. Responses indicate a positive relationship between hiring and human resources (HR) recruitment efforts, reflected by the five-percentage-point increase from last year in those who feel their HR department frequently or always understands cybersecurity hiring needs.

Seventy-one percent of survey respondents claim their organizations have unfilled cybersecurity positions regardless of type (**figure 7**). Surveys in prior years did not permit respondents to distinguish between entry-level and non-entry-level vacancies;[14] for 2023, respondents were asked about both. As shown in **figure 7**, the percentage of unfilled non-entry-level openings outnumbers the percentage of unfilled

FIGURE 6: Comprehension of Hiring Needs by HR

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

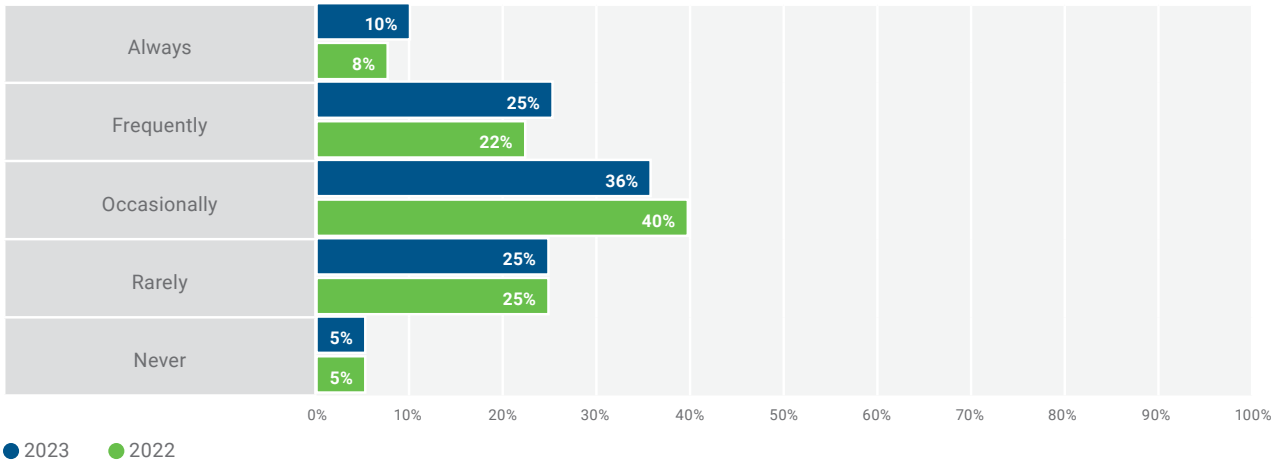
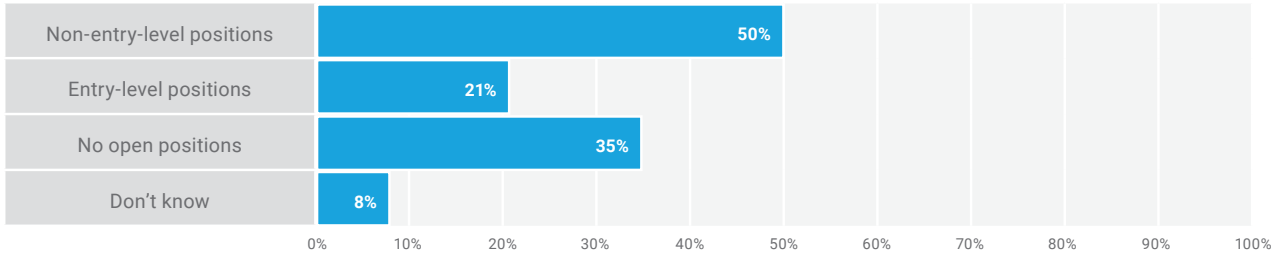


FIGURE 7: Unfilled Positions

Does your organization have unfilled (open) cybersecurity positions? Select all that apply.



14 In 2022, 63 percent of respondents answered "Yes" to the question, "Does your organization have unfilled (vacant) positions?"

entry-level openings by more than two to one. Also of interest, those who reported "No open positions" increased six percentage points from last year.

Time to fill non-entry-level positions is more challenging, with 67 percent of respondents indicating their organizations take at least three months to fill these roles (**figure 8**).

Technical nonsupervisory cybersecurity positions remain the top vacancy category again this year (**figure 9**). However, a notable decline of at least three percentage points across all categories is illustrated in year-over-year data (**figure 10**).

Technical nonsupervisory cybersecurity positions remain the top vacancy category again this year.

FIGURE 8: Time to Fill Cybersecurity Positions

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

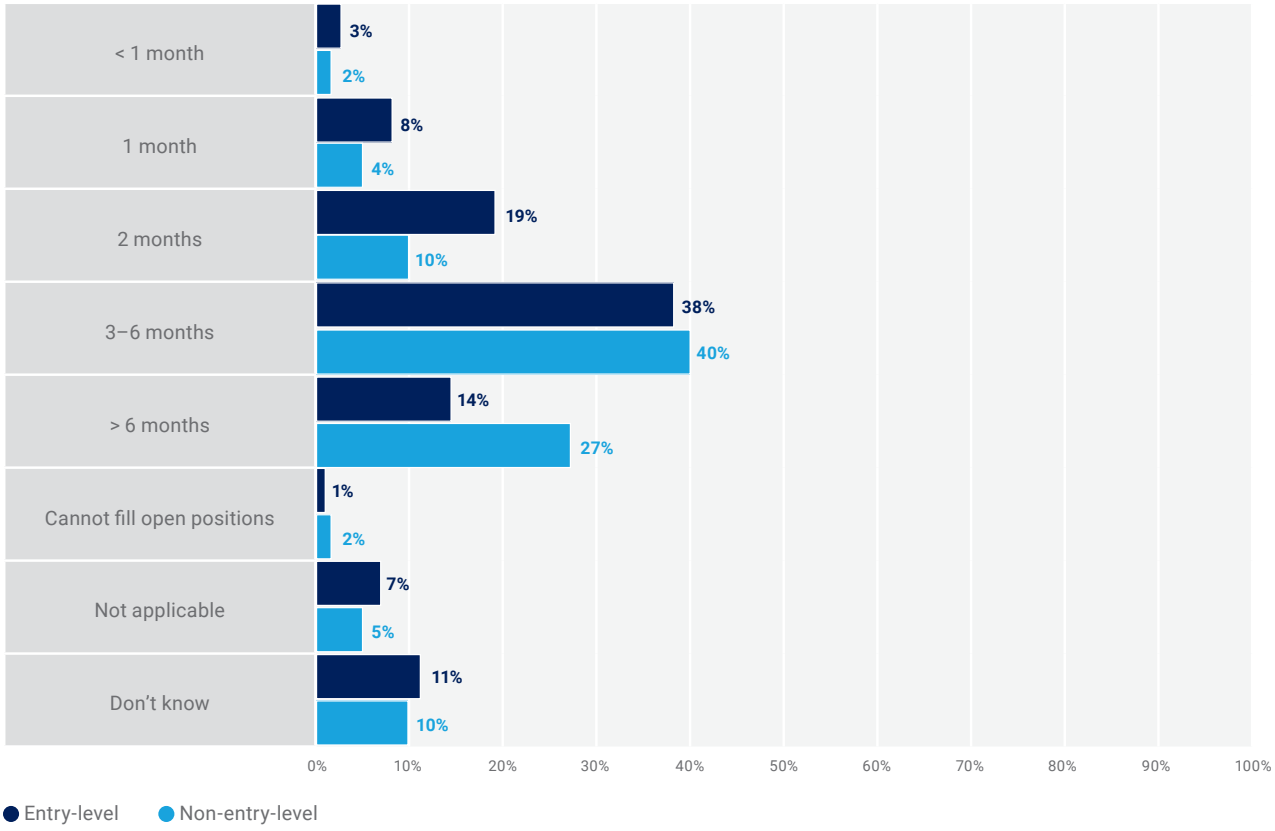


FIGURE 9: Percentages of Unfilled Positions at Given Organizational Levels

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

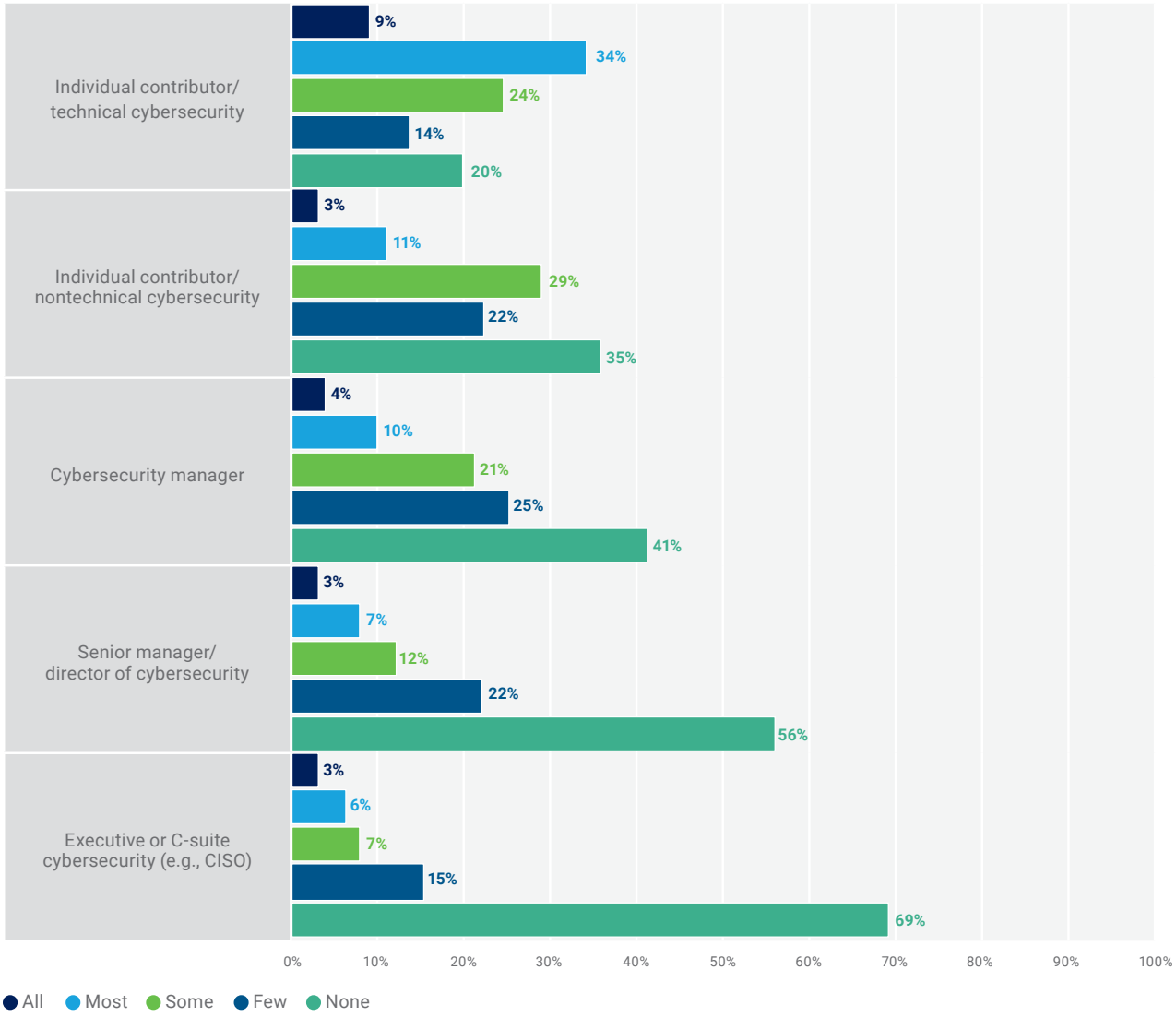
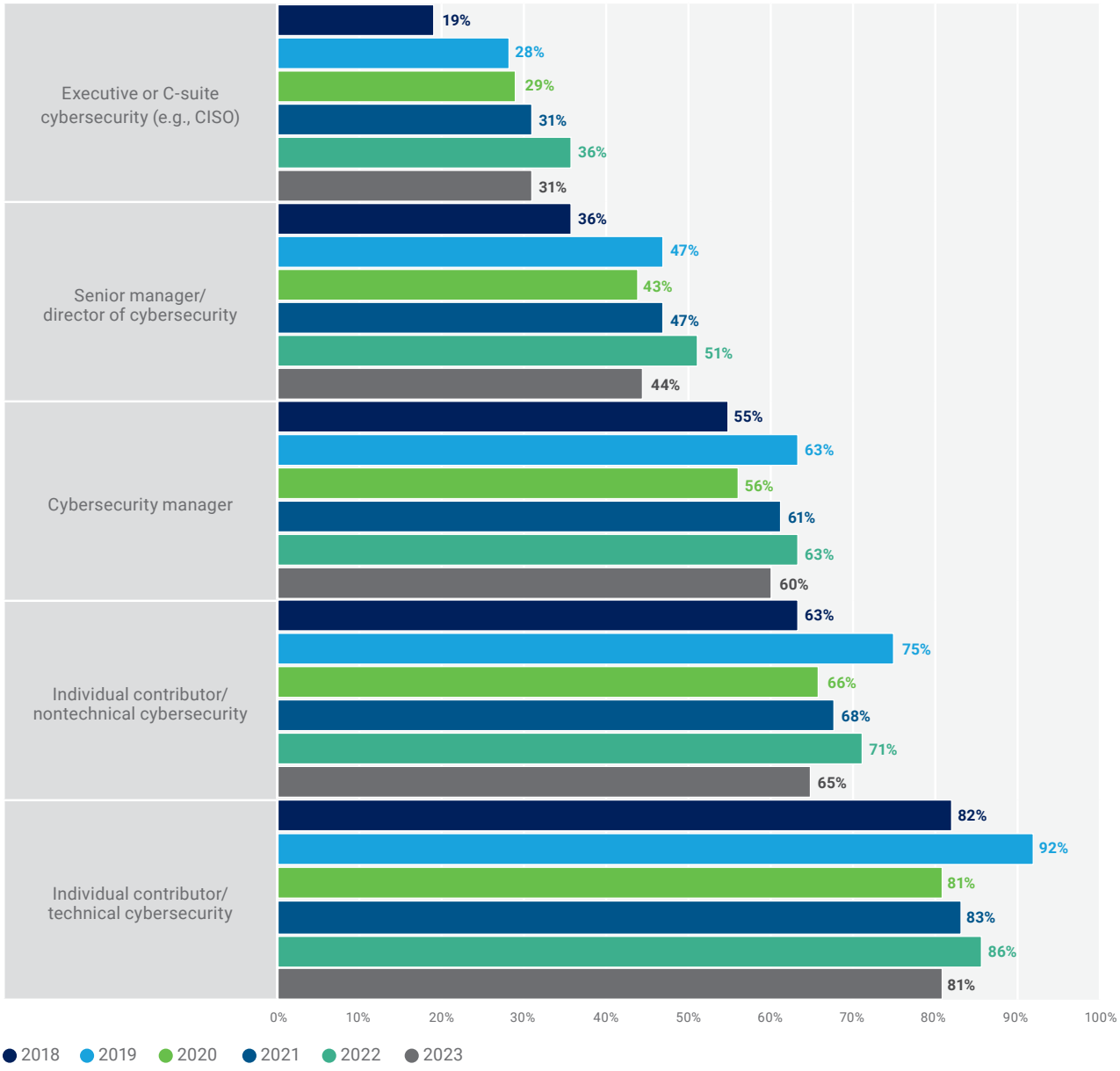


FIGURE 10: Unfilled Position Reporting (2018-2023)[15]



15 This figure compares data on unfilled positions from ISACA *State of Cybersecurity* surveys from 2018 to 2023. Percentages represent the sum of all reported vacancy percentages for each position and exclude the "None" responses.

Regarding future demand (**figure 11**), respondent views reveal skepticism about addressing current shortfalls, with a notable decrease in demand predicted across all categories. **Figure 12** includes six years of data, with 2023 showing indications that last year's spike was anomalous.

Retention

After last year's spike in difficulty retaining talent, ISACA *State of Cybersecurity 2023* survey data show respondents observed less difficulty (56 percent) retaining qualified cybersecurity professionals in 2023, a four-percentage-point decrease from 2022 (60 percent).

The reasons behind cybersecurity professionals' decisions to leave their jobs vary from a year ago (**figure 13**). Recruitment by other companies remains the largest perceived reason cybersecurity professionals leave positions (58 percent). But the second highest response, poor financial incentives (e.g., salaries or bonuses), is likely the main driver. Those seeking better financial compensation

FIGURE 11: Future Hiring Demand

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

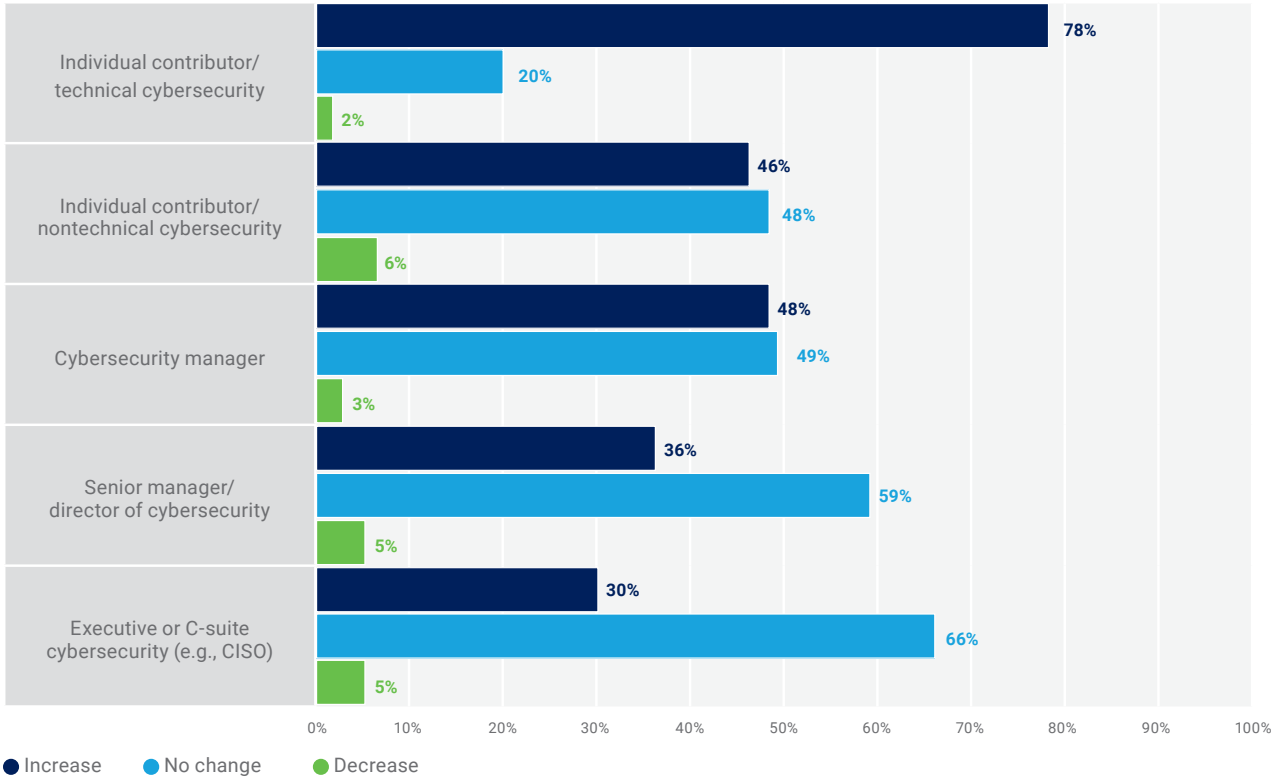
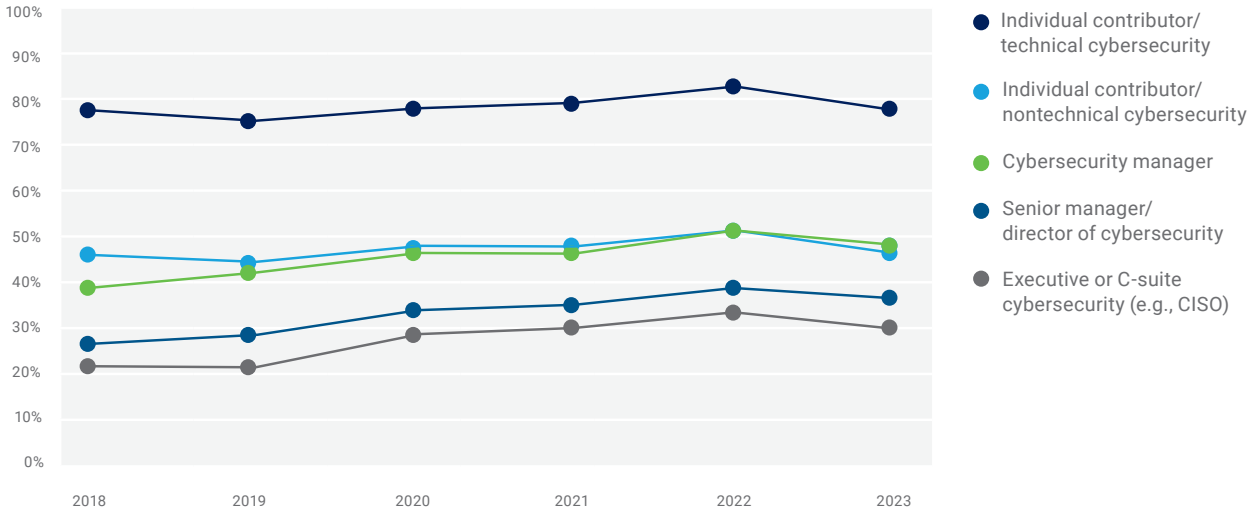


FIGURE 12: Hiring Demand Trending (2018-2023)



increased by six percentage points from last year to 54 percent. While high work stress levels dropped by two percentage points from 2022, it remains a contributing factor at 43 percent, ranking fourth in the list. Other notable reasons include limited remote work possibilities (increased by four percent from last year) and poor work culture/environment, both potentially driven by return-to-work mandates. Limited promotion and development opportunities remained largely unchanged, as did retirement, lack of workplace diversity and switching careers.

Erosion of Employer Benefits

Economic uncertainty may be driving reductions in employer benefits. If true, this might adversely affect retention and an enterprise's ability to defend critical business functions and data. University tuition reimbursement dropped five percentage points from 2022 to 28 percent. Recruitment bonuses fell two percentage points this year, while reimbursement of certification fees dropped by one percentage point. Certification maintenance/renewal and signing bonuses remain unchanged. Paid volunteer time off rose slightly to 21 percent. The percentage of respondents (56 percent) indicating employers offer a flexible work schedule remains unchanged from last year (**figure 14**).

Continuing education requirements often fall on the employee, and conscious decisions to not reimburse certified practitioners are an additional stressor to some employees.

A large gap remains between employers paying employee certification fees and the associated maintenance/renewal fees. As is, continuing education requirements often fall on the employee, and conscious decisions to not reimburse certified practitioners are an additional stressor to some employees.

FIGURE 13: Why Cybersecurity Professionals Leave Their Jobs

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

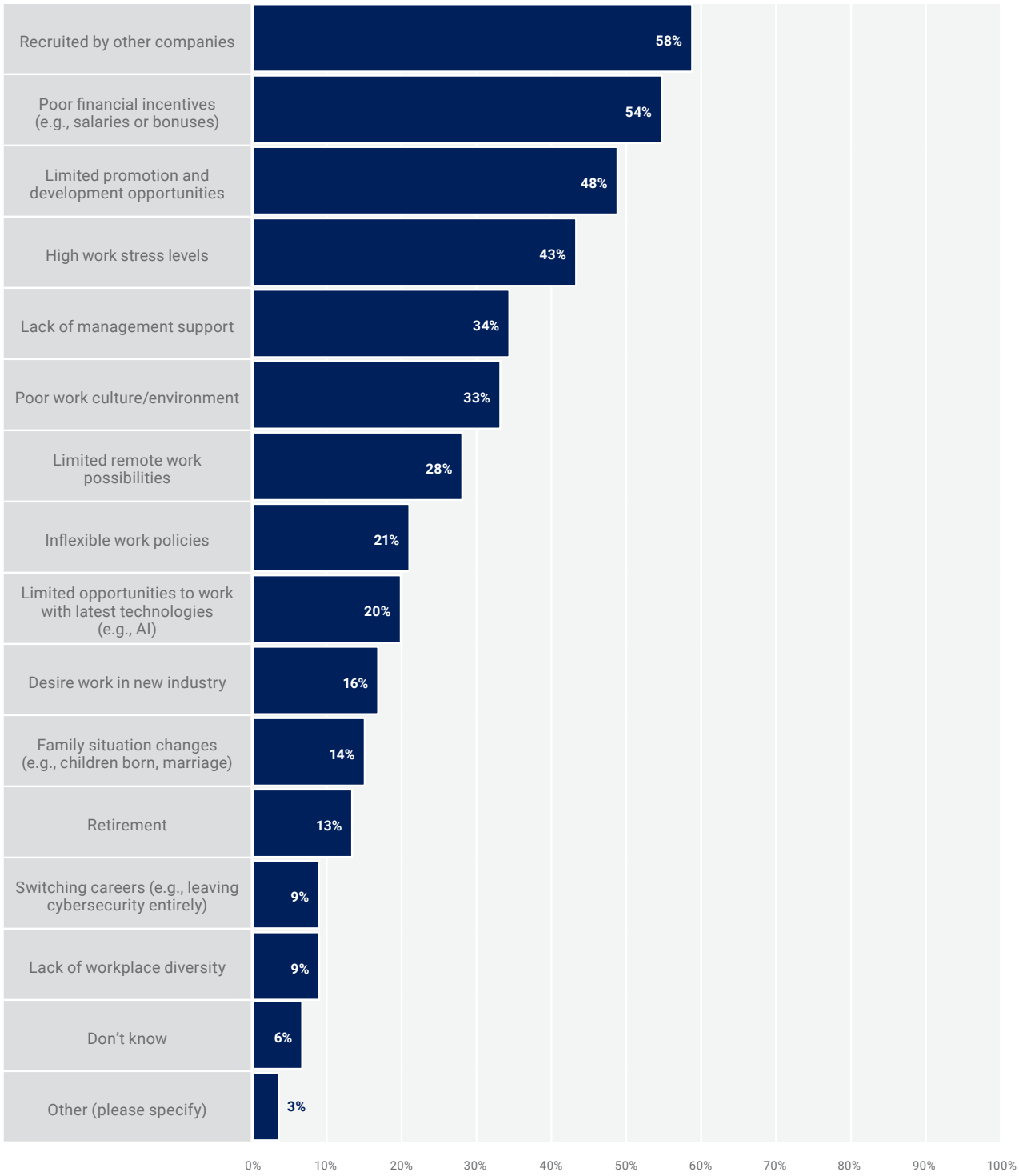
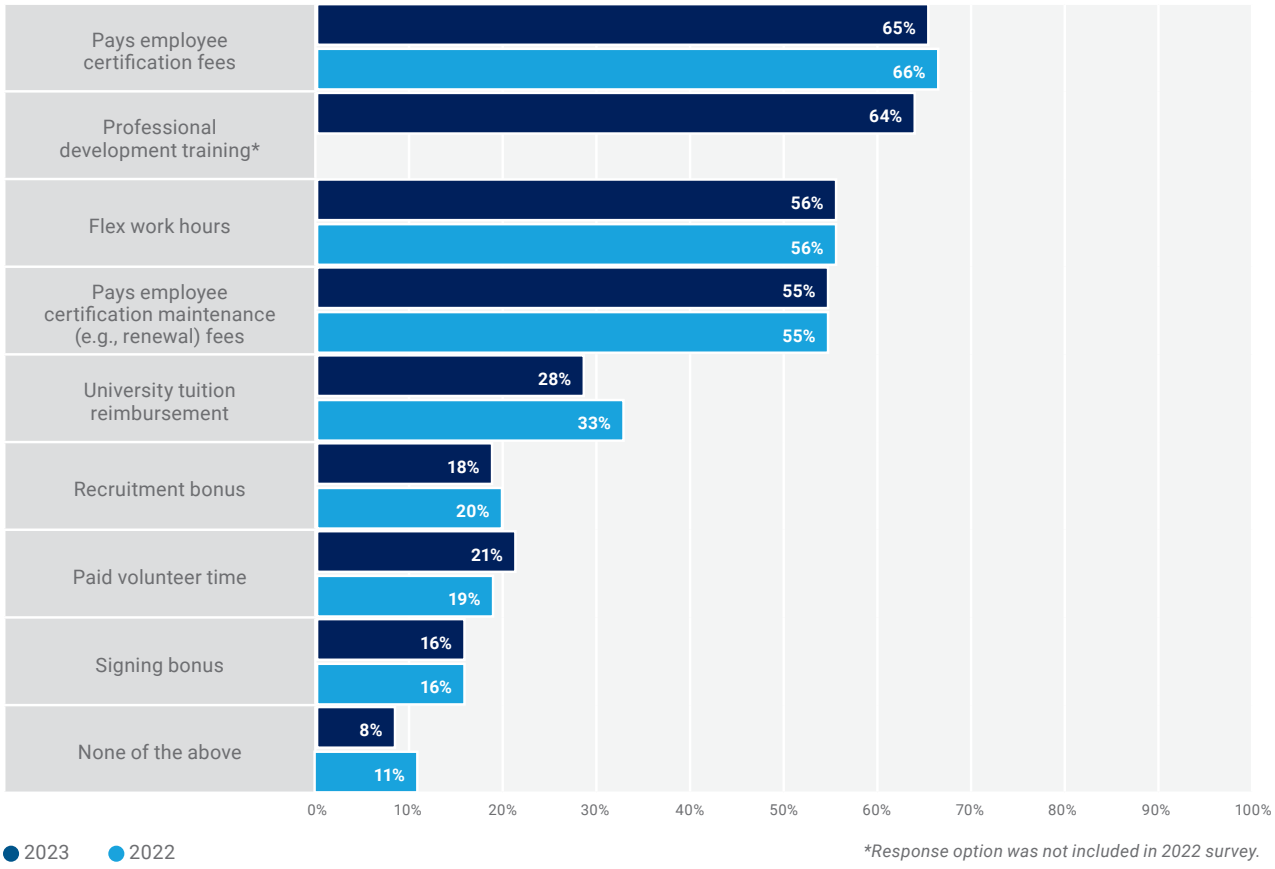


FIGURE 14: Employer Benefits

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



**Response option was not included in 2022 survey.*

Deep Dive Into Pipeline Issues

Hiring managers continue to have low confidence in cybersecurity applicants' qualifications—a theme carried forward for several years now. **Figure 15** shows that just 26 percent of those surveyed believe at least half of applicants are well qualified.

Figure 16 shows that prior hands-on cybersecurity experience remains the primary factor (72 percent) in determining whether a candidate is qualified—with no statistically significant change from 2022. The largest skill gap continues to be soft skills (**figure 17**).

Survey responses indicate that cloud computing is the second-largest skill gap among cybersecurity professionals (47 percent), just behind soft skills (55 percent). Other notable gaps include security controls

FIGURE 15: 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?

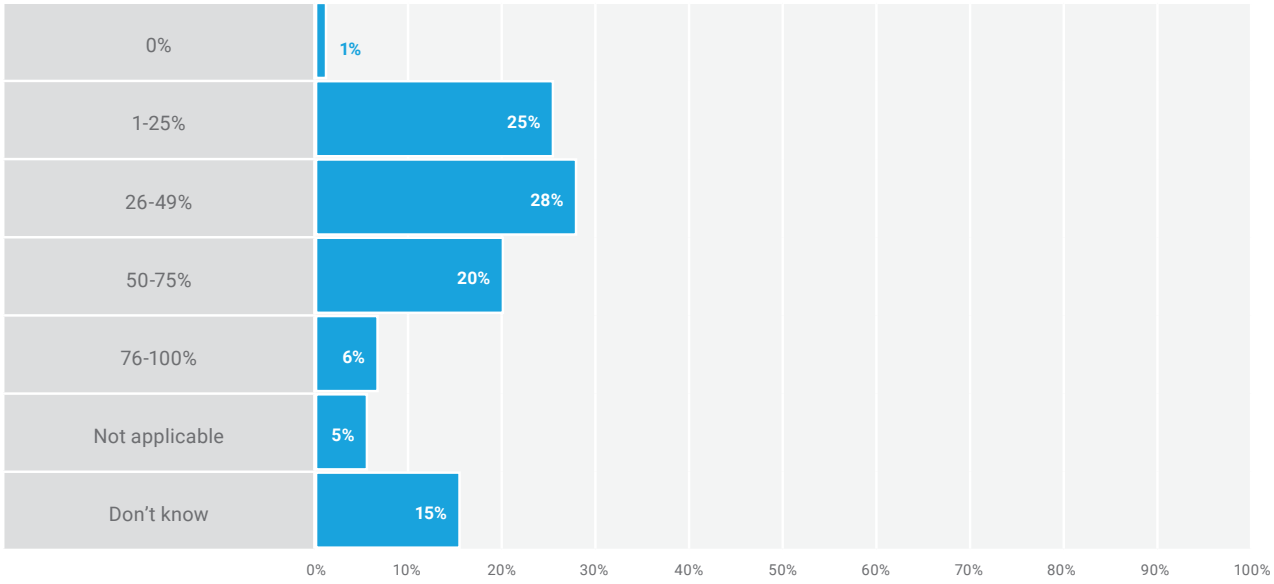


FIGURE 16: Candidate Qualifications

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

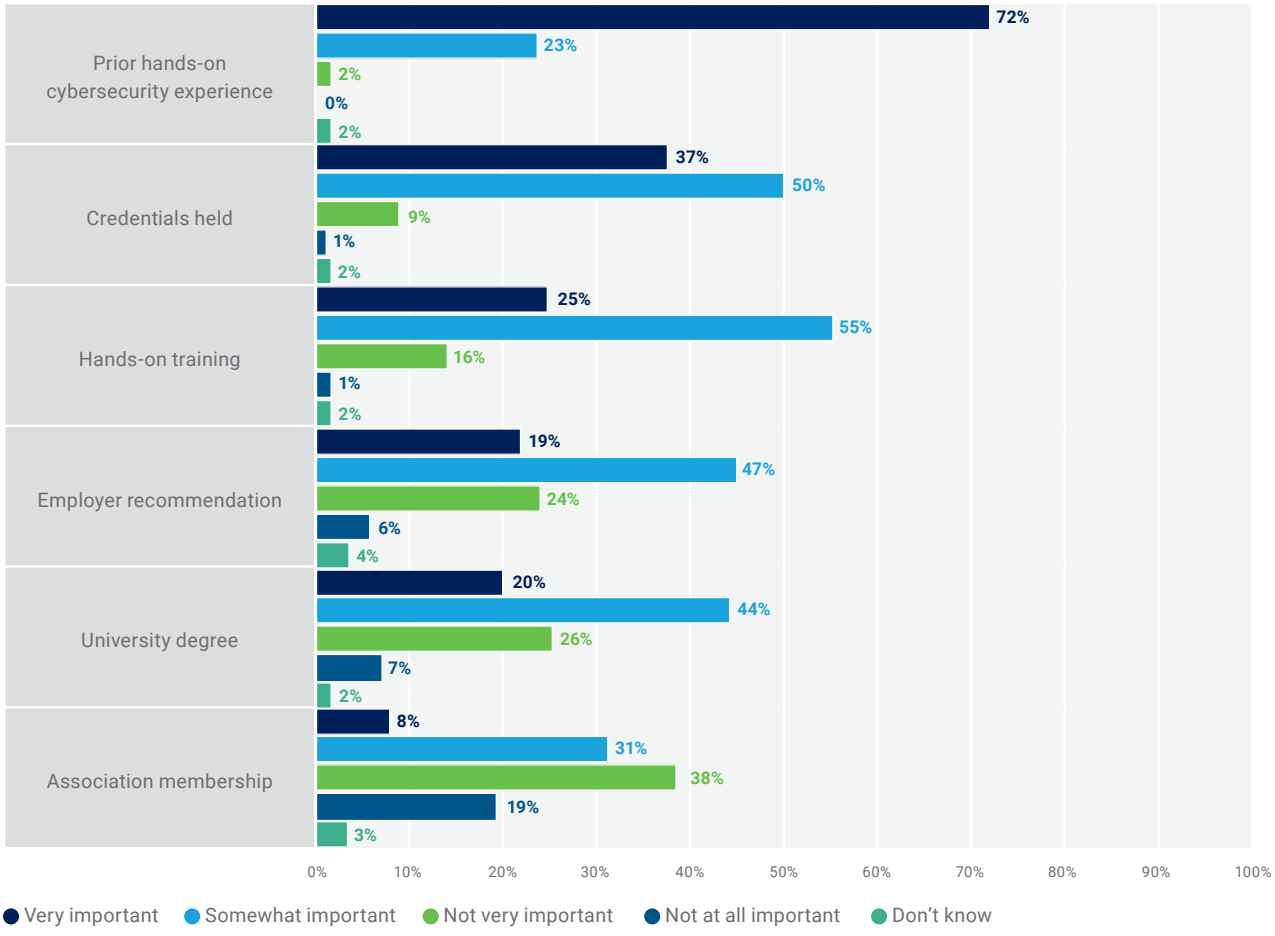
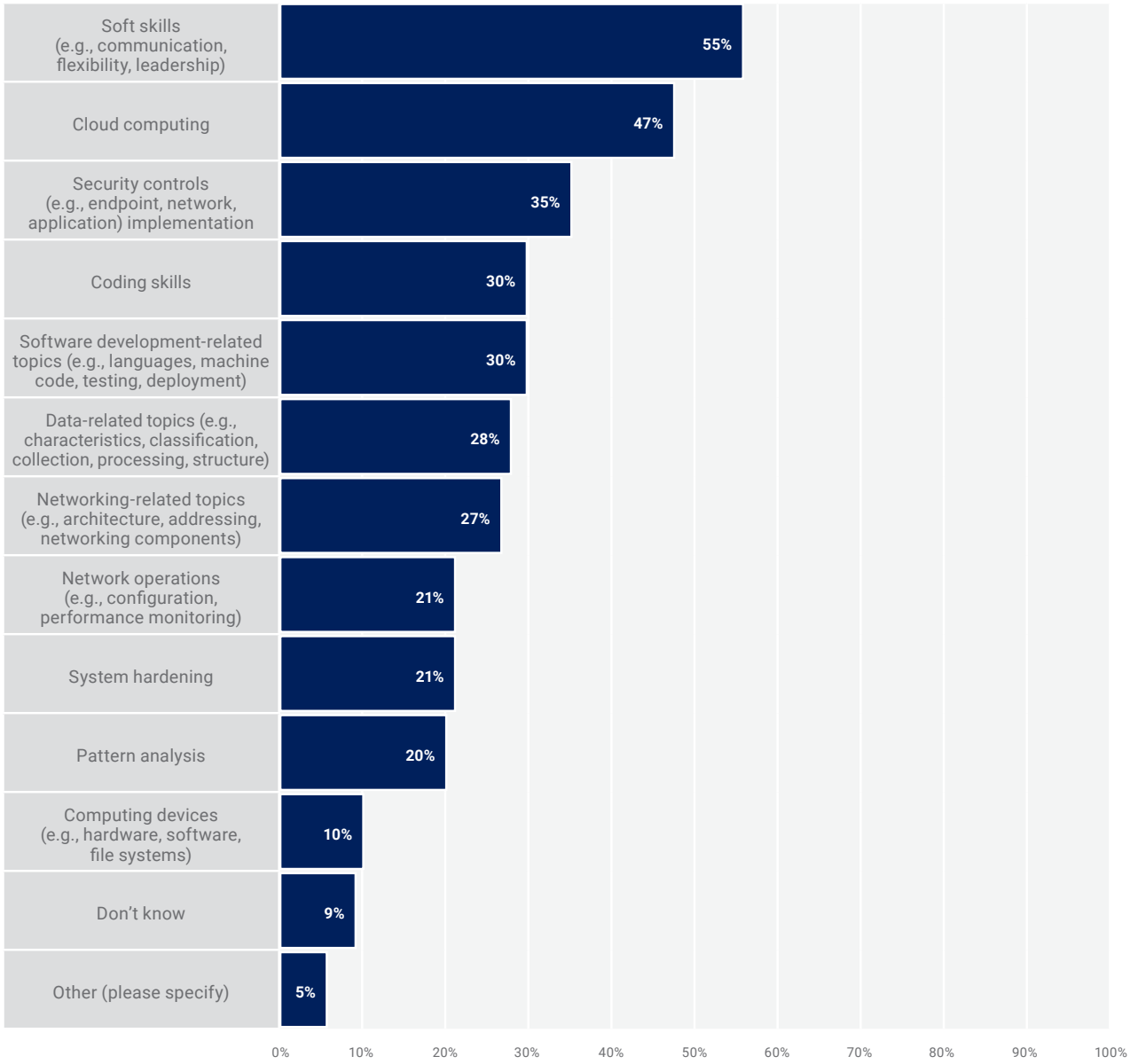


FIGURE 17: Quantified Skills Gaps

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



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).

University Insights

Despite industry trends that indicate large numbers of practitioners hold academic degrees,[16] respondents' opinions on the preparedness of recent university graduates for organizational cybersecurity challenges remain critical, with no notable change from the previous year (**figure 18**). The percentage of organizations requiring a degree to fill entry-level cybersecurity positions remains consistent at 52 percent (**figure 19**); however, the persistent shortfalls in technical and soft skills competencies noted among recent university graduates challenge the effectiveness of cybersecurity degree programs to meet the needs of employers (**figure 20**).

Survey data continue to emphasize a soft skills deficit (68 percent) among recent graduates. While many of the technical skills deficits reported this year are similar to last year, skills gaps in networking-related and data-related topics were four and two percentage points higher, respectively, than last year (**figure 20**).

FIGURE 18: 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?

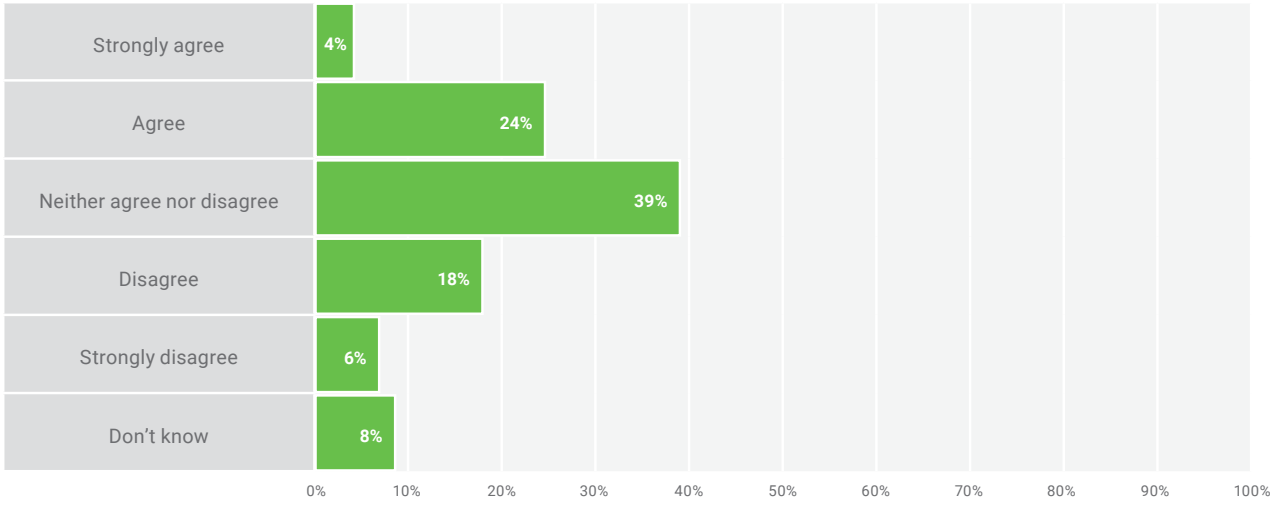
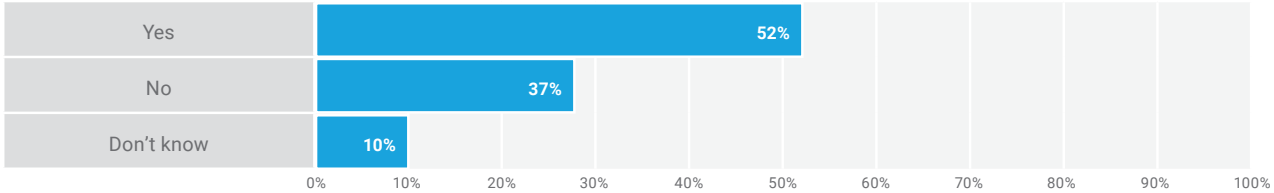


FIGURE 19: University Requirement

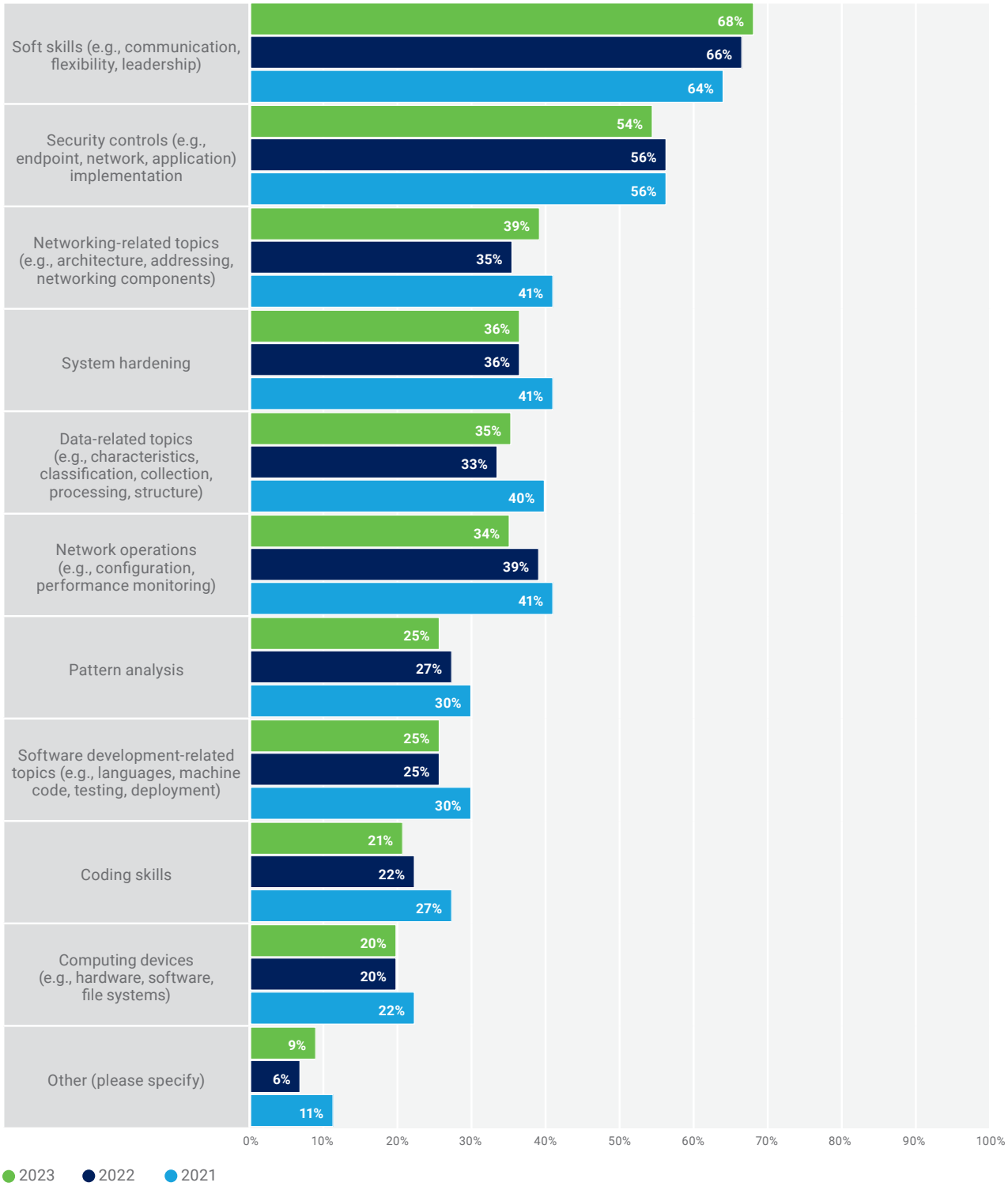
Does your organization typically require a university degree to fill your entry-level cybersecurity positions?



16 ISC2, "(ISC)2 Cybersecurity Workforce Study, 2022," https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf

FIGURE 20: Skill Gaps Among Recent Graduates

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



Although the overall percentage of enterprises requiring university degrees for entry-level cybersecurity positions remains unchanged from a year ago, variations across geographical regions are noticeable. The decline in organizations requiring a university degree continues in Europe, dropping by five percentage points from 2022 and 11 percentage points since 2021. The European Union Agency for Cybersecurity (ENISA) efforts, such as the European Cybersecurity Skills Framework (ECSF) and Cybersecurity Higher Education Database (CyberHEAD), may be influencing this trend, especially when considering the minimum standard for approval of a bachelor degree program requires just 25 percent of modules to be in cybersecurity topics.[17] Africa also saw a slight decline in university degree requirements for entry-level positions (69 percent in 2023 vs. 71 percent in 2022), while Asia and North America saw no meaningful change from a year ago. Latin America respondent data reversed last year's downward trend, reaching 70 percent—an increase of 9 percentage points. Lastly, Oceania also noted a 10-percentage-point hike from 2022 (37 percent).

Qualifying Workforce Issues

This year's data saw some shifts in the perceived importance of different security skills within organizations. Cloud computing decreased by four percentage points and moved below identity and access management (IAM), which was ranked as the top security skill (**figure 21**). Data protection fell by three percentage points (44 percent) but retained its ranking as the third most important security skill. Data collection and correlation saw a slight increase to 33 percent.

The top five most important soft skills are still communication, critical thinking, problem solving, teamwork and attention to detail (**figure 22**). Communication (both listening and speaking) remains the top soft skill security professionals need, according to 58 percent of respondents. The low rankings of empathy (13 percent) and, in particular, honesty (17 percent) should concern enterprise leadership who want to successfully navigate the ever-changing regulatory landscape, given that 62 percent of survey respondents believe organizations underreport cybercrime.

Early Career Staff Insights

ISACA sought data on the readiness of security staff with less than three years of work experience, which is especially important given the aging workforce. The top four reported training areas for security staff with less than three years of work experience were unchanged from last year, but soft skills (e.g., communication, critical thinking, flexibility and leadership) increased by three percentage points, nearly matching security controls (**figure 23**).

Human Capital Mitigations

Cross-training nonsecurity professionals for security roles remained the top means of mitigation for employers trying to address technical shortfalls and skills gaps (**figure 24**). The use of contractors and consultants dropped by four percentage points, while reliance on artificial intelligence (AI) or automation decreased by six percentage points, becoming the fifth most popular skill-gap mitigation method. The explosion of generative AI tools such as ChatGPT (and the associated risk) may have influenced this decline after its steady year-over-year climb in the rankings.

Cross-training nonsecurity professionals for security roles remained the top means of mitigation for employers trying to address technical shortfalls and skills gaps.

Employer actions to overcome soft skills shortcomings are illustrated in **figure 25**; one notable change shows a decrease in academic tuition reimbursement by four percentage points from last year.

17 ENISA, "CYBERHEAD - Cybersecurity Higher Education Database," https://www.enisa.europa.eu/topics/education/cyberhead/#/faq

FIGURE 21: Top Five Security Skills

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

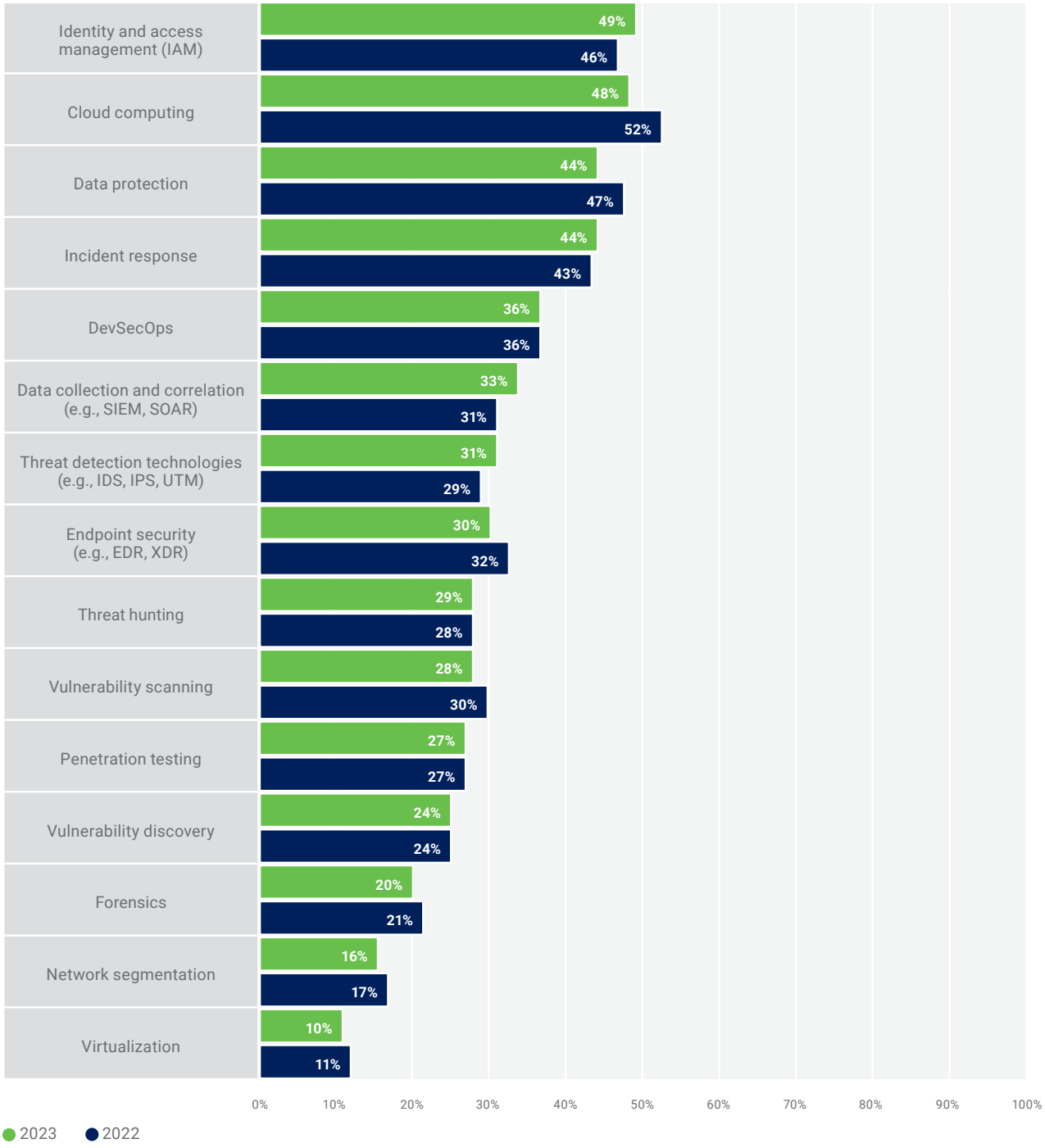


FIGURE 22: Top Five Soft Skills

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

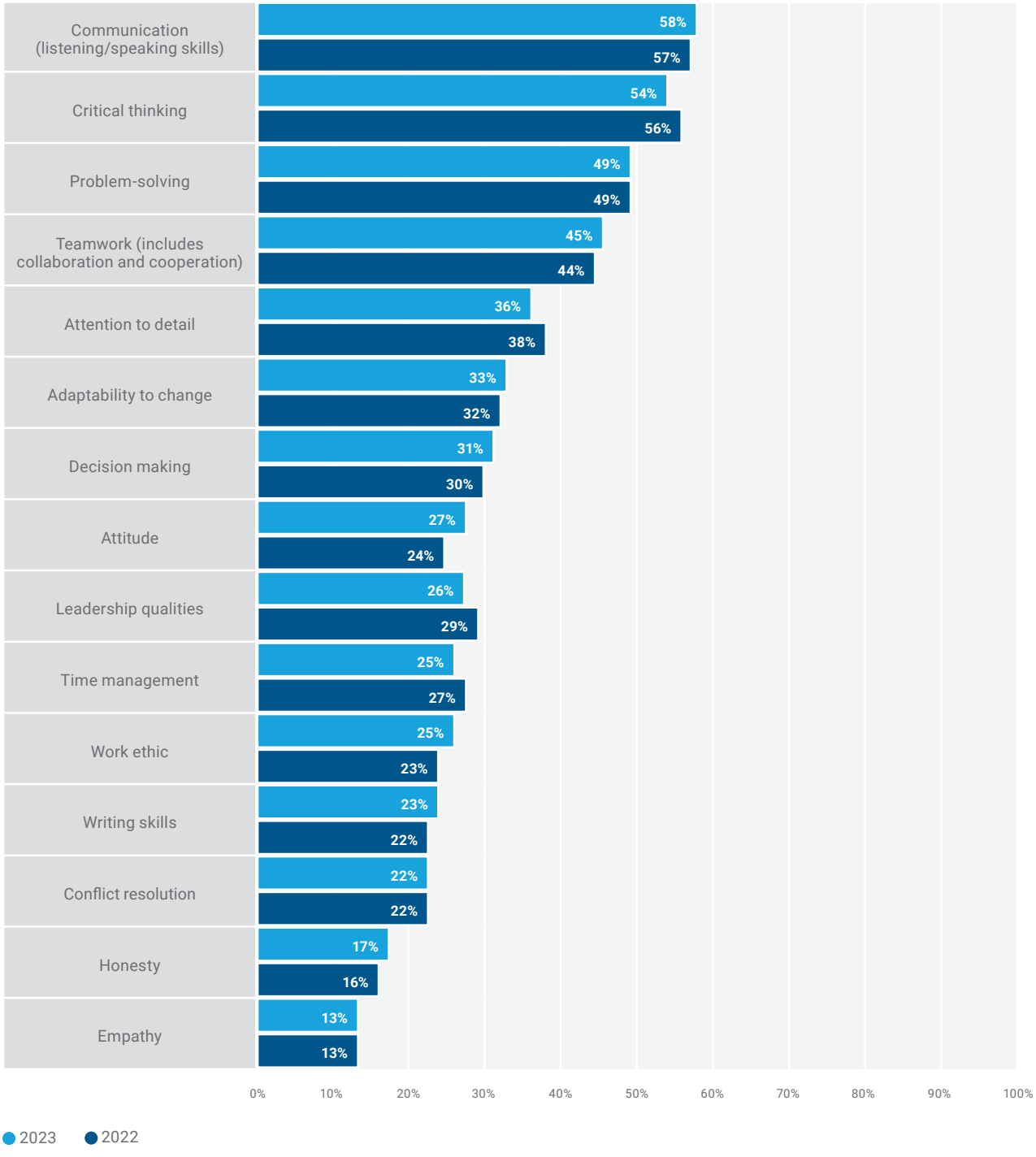


FIGURE 23: Professional Development Needs for Staff With Less Than Three Years Experience

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

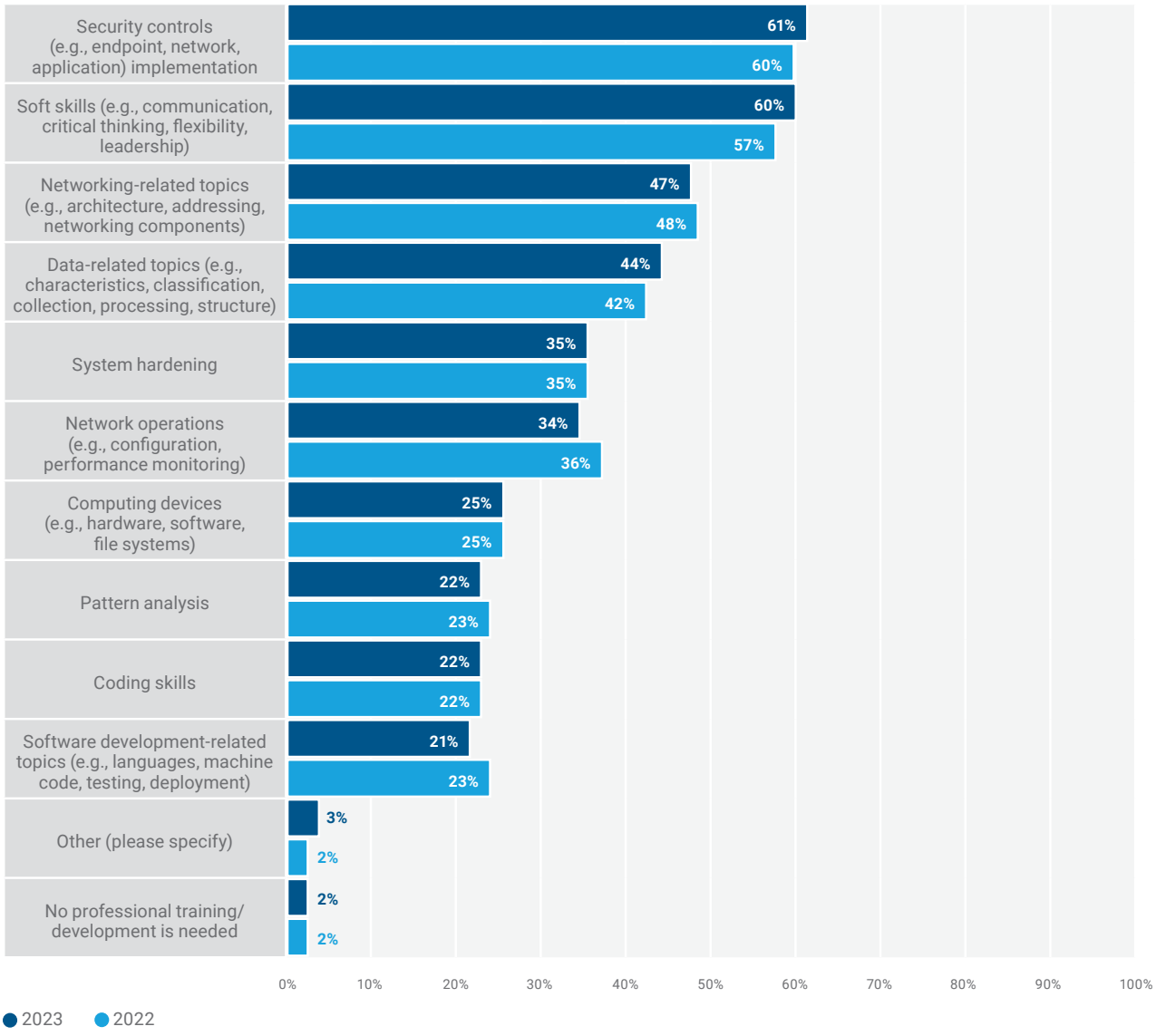
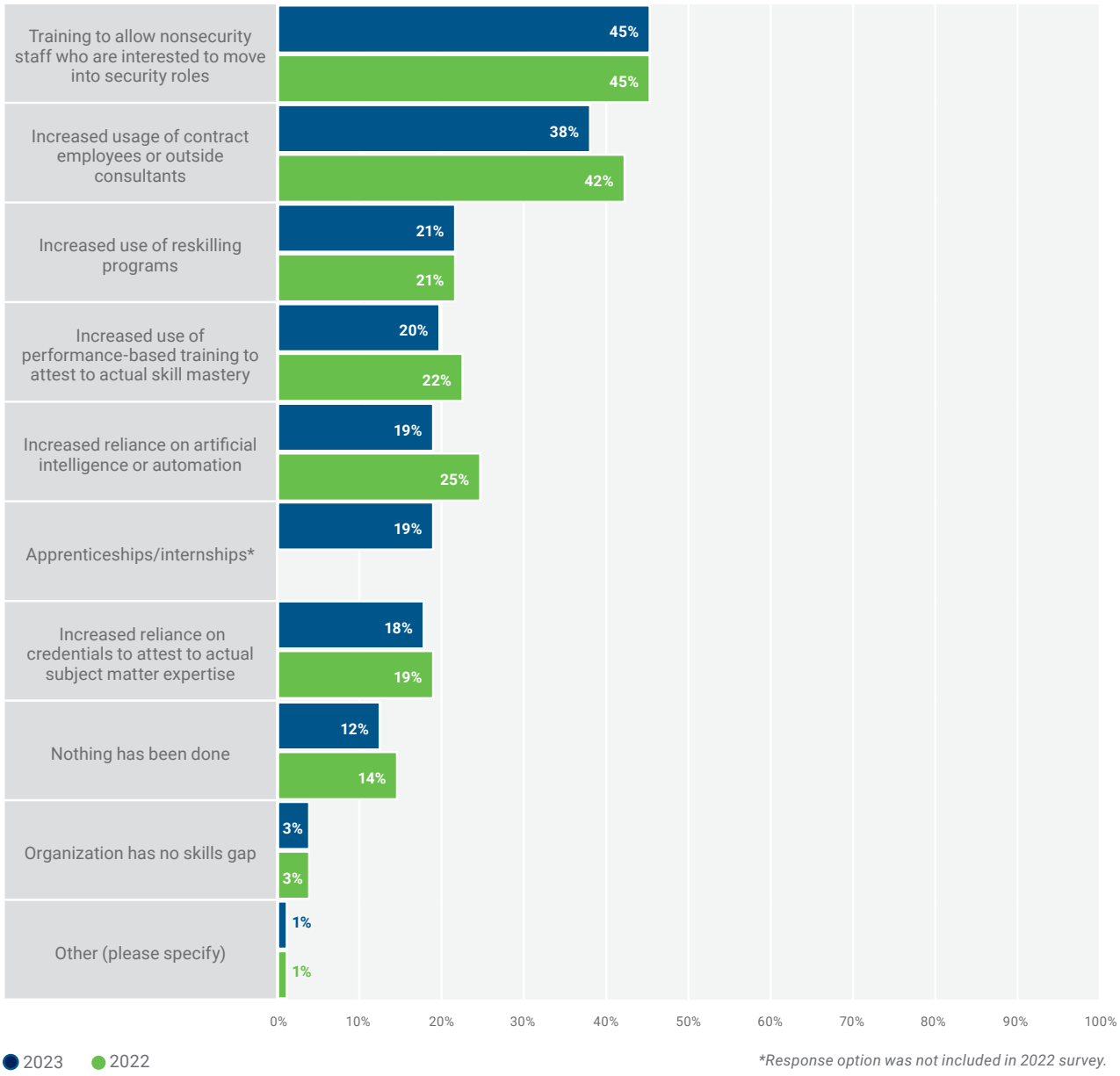


FIGURE 24: Means of Mitigating Technical Skills Gaps

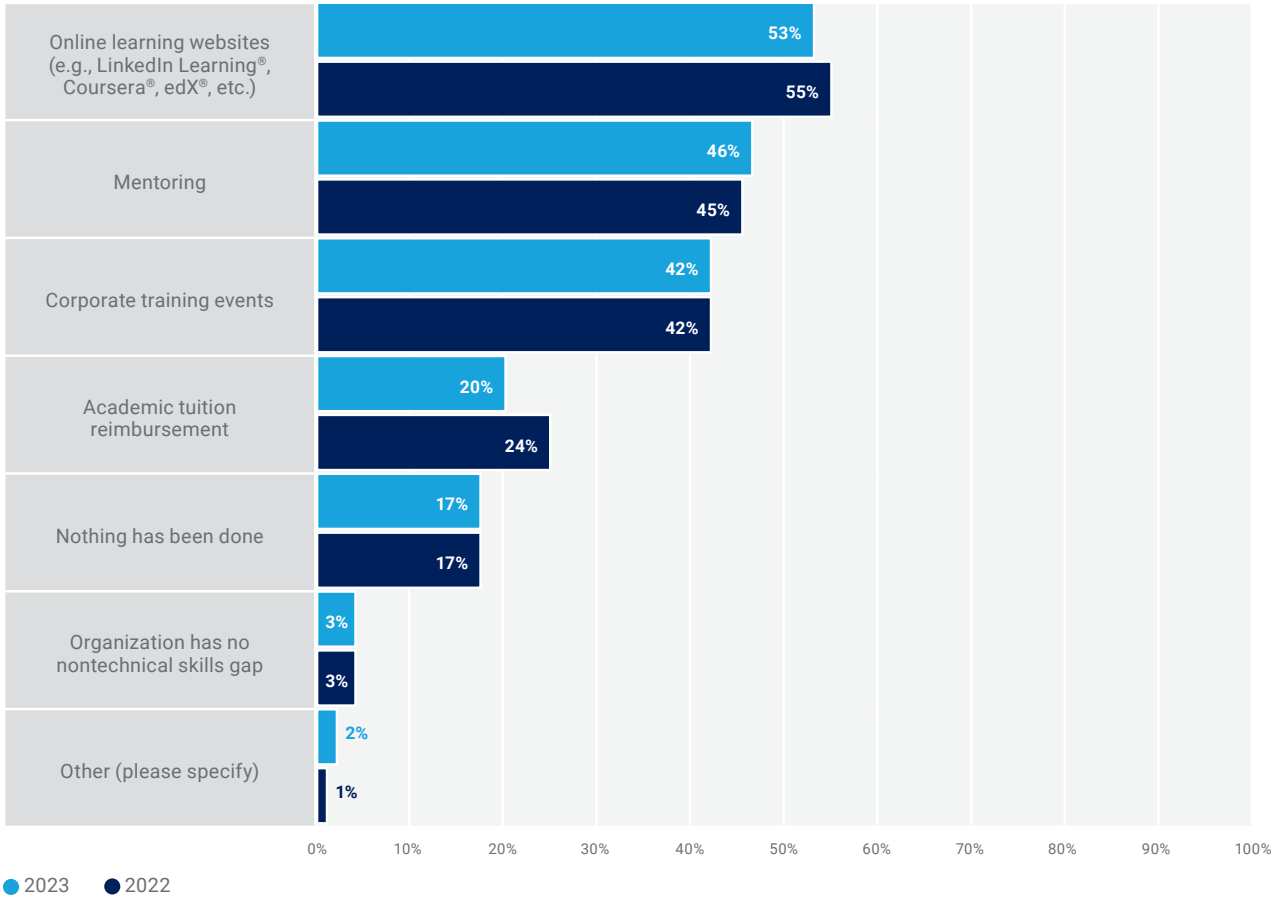
Which, if any, of the following has your organization undertaken to help decrease technical cybersecurity skills gaps? Select all that apply.



**Response option was not included in 2022 survey.*

FIGURE 25: 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 Threatened

Survey respondents' views on cybersecurity funding (**figure 26**) remain unchanged from a year ago, with the data showing no statistical difference. Respondents generally believe cybersecurity budgets will taper off (**figure 27**), but the budget outlook for cybersecurity funding in 2024 continues its biannual up-and-down cycle, dipping to its lowest point since 2017 (**figure 28**). Multiyear data support previous reporting that says budgets have leveled out.

FIGURE 26: Cybersecurity Funding Perception

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

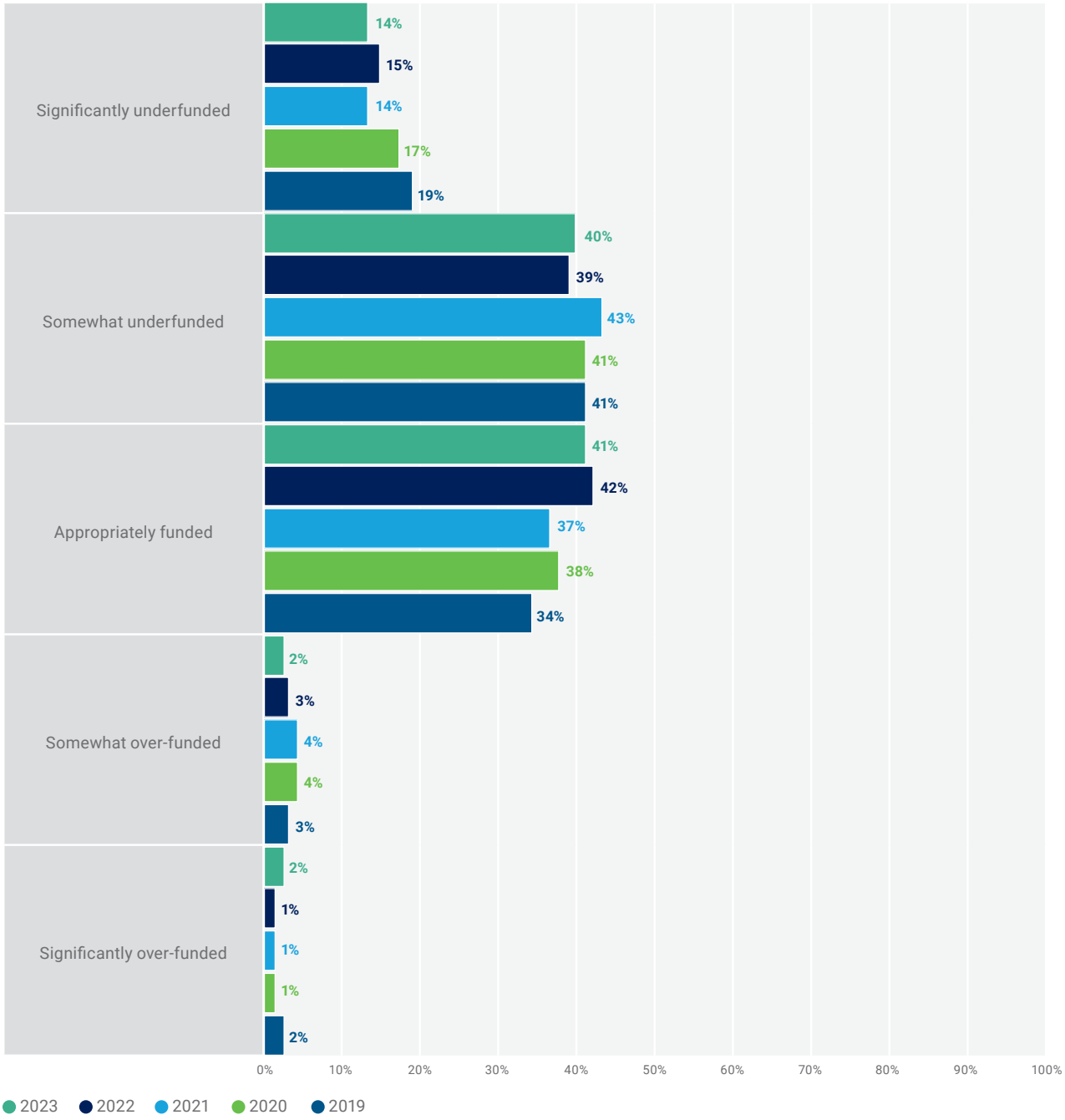


FIGURE 27: Enterprise Security Budget Outlook

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

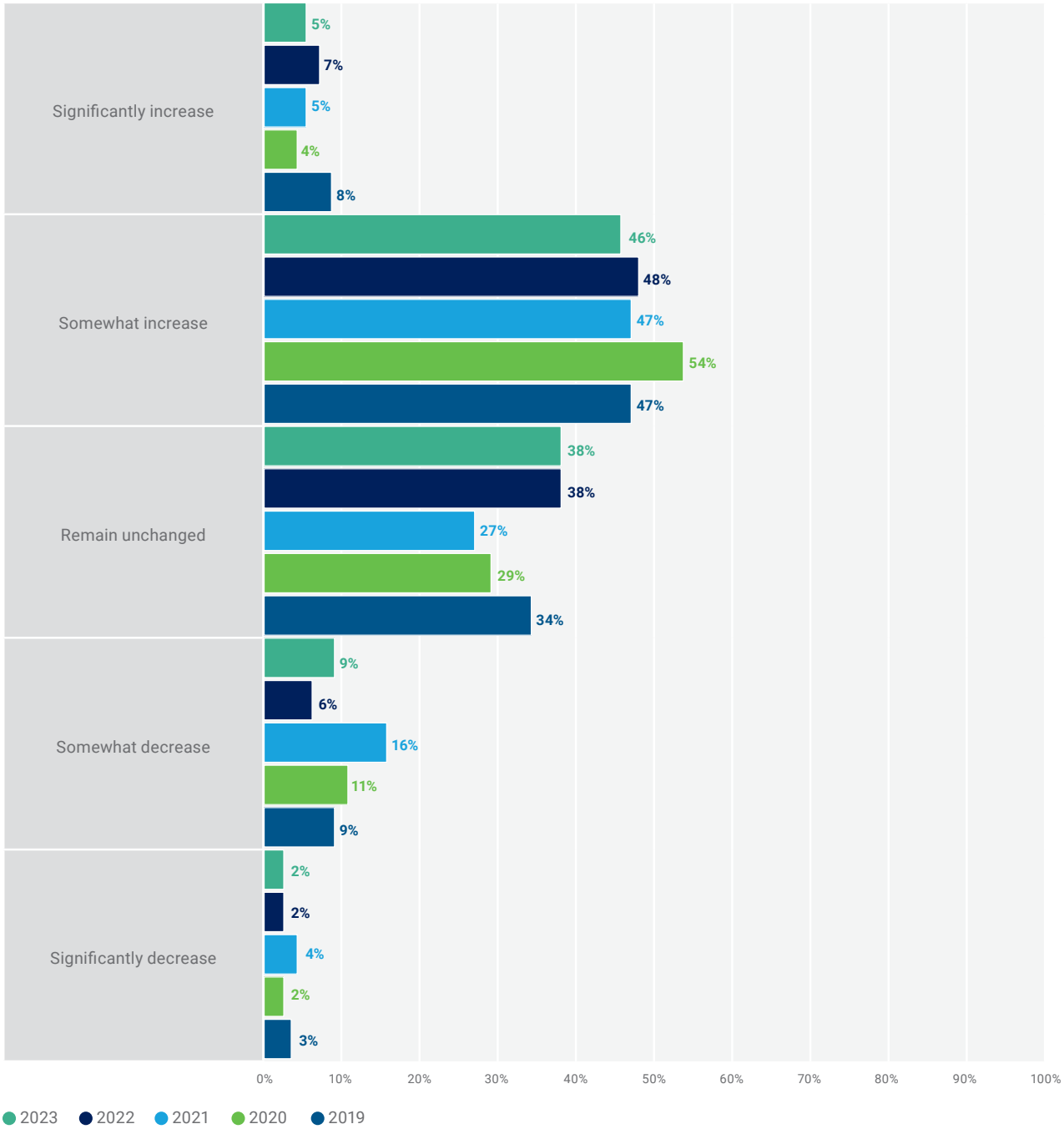
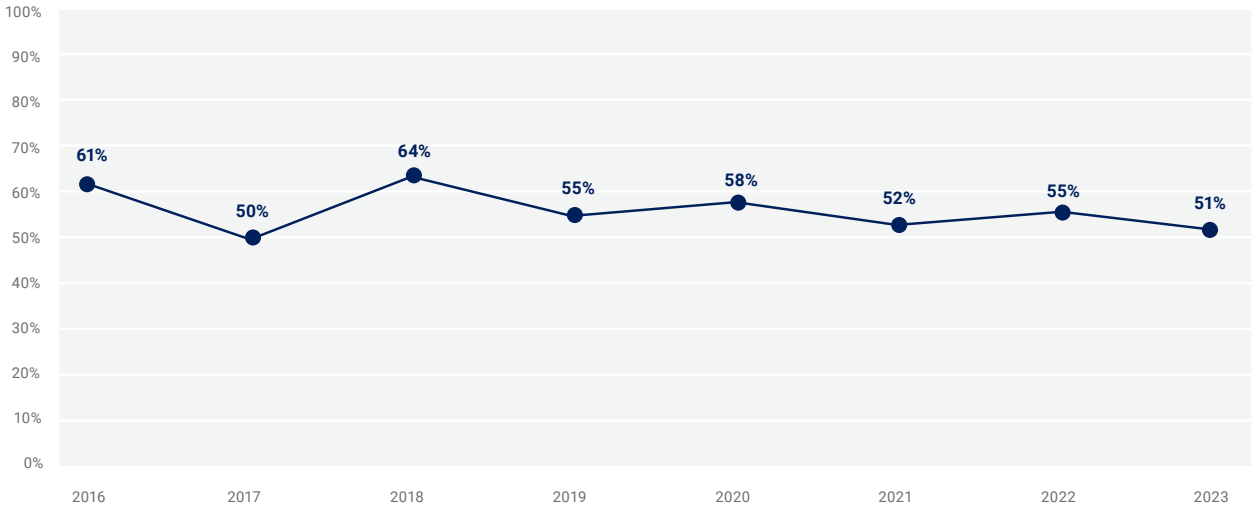


FIGURE 28: Forecasted Security Budget Increases (8 Year)



Threat Landscape

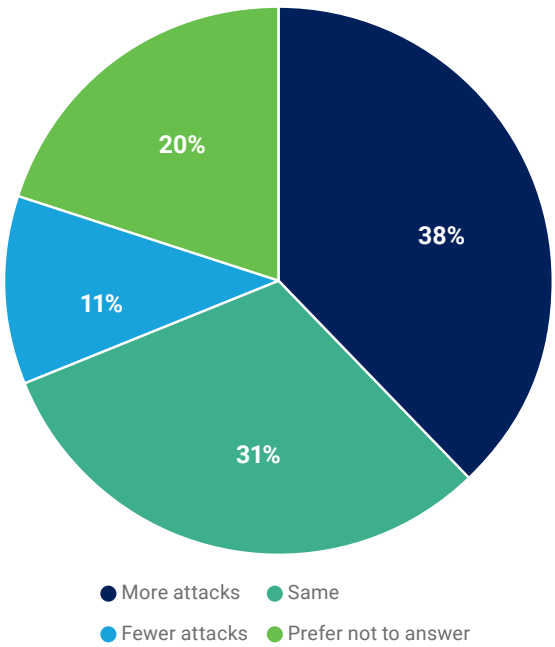
Thirty-eight percent of respondents indicate that their organization is experiencing more cyberattacks than a year ago (**figure 29**), a five-percentage-point decrease from last year. There was an equal drop in respondents who believe it is likely or very likely that their organization will experience a cyberattack in the coming year (**figure 30**).

This is the most optimistic view since ISACA began collecting these data, bolstered by an increase in those who believe the number of cybersecurity attacks remained the same.

It is likely this trend may reverse next year given the timing of the MOVEit exploit,[18] an evolving cybercrime-as-a-service[19] model, the pervasiveness of business email compromise[20] and the nefarious use of large language models (LLMs).[21]

FIGURE 29: Change in Number of Cybersecurity Attacks

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



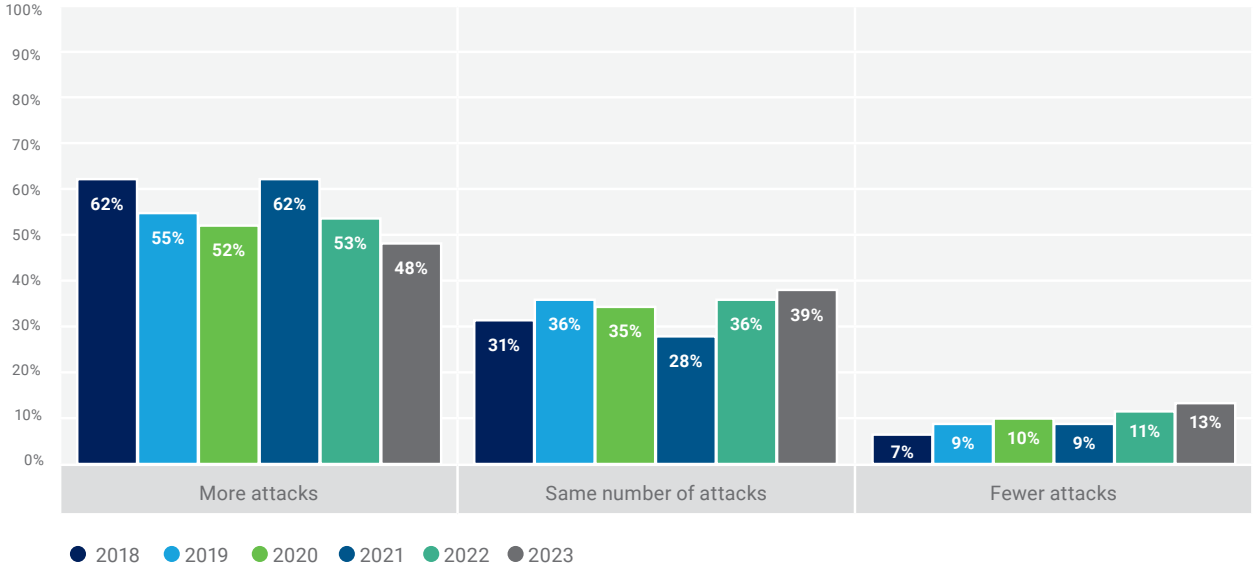
18 Kapko, M.; "MOVEit mass exploit timeline: How the file-transfer service attacks entangled victims," Cybersecuritydive.com, 14 July 2023, https://www.cybersecuritydive.com/news/moveit-breach-timeline/687417/

19 Hong Kong Computer Emergency Response Team (HKCERT), "Unmasking Cybercrime-as-a-Service: The Dark Side of Digital Convenience," 15 May 2023, https://www.hkcert.org/blog/unmasking-cybercrime-as-a-service-the-dark-side-of-digital-convenience

20 Microsoft, "Shifting tactics fuel surge in business email compromise," 19 May 2023, https://www.microsoft.com/en-us/security/business/security-insider/reports/cyber-signals/shifting-tactics-fuel-surge-in-business-email-compromise

21 Verizon, "2023 Data Breach Investigations Report," https://www.verizon.com/dbir; Dresp-Langley, B.; "The weaponization of artificial intelligence: What the public needs to be aware of," *Frontiers in Artificial Intelligence*, vol. 6, 8 March 2023, https://www.frontiersin.org/articles/10.3389/frai.2023.1154184/full; TheHackerNews.com, "New AI Tool 'FraudGPT' Emerges, Tailored for Sophisticated Attacks," 26 July 2023, https://thehackernews.com/2023/07/new-ai-tool-fraudgpt-emerges-tailored.html

FIGURE 30: Year-Over-Year Comparison of Cybersecurity Attack Reporting[22]



Detection and Monitoring Confidence

Survey respondents' confidence in the ability of their cybersecurity teams to detect and respond to cyberthreats remains nearly unchanged from last year at 81 percent[23] (**figure 31**); this is remarkable considering 47 percent of respondent enterprises have a security staff of just two to 10 individuals. This year, data reveal that in-house staff fully perform over half of the five major security functions (identify, protect, detect, respond and recover).

Cybersecurity education and awareness training programs continue to positively impact overall employee awareness, with 81 percent[24] of survey respondents reporting at least some positive impact (**figure 32**).

Threat Actors and Attacks

The top three cyberattack concerns of respondents remain unchanged for the fourth consecutive year (**figure 33**):

- Enterprise reputation (79 percent)
- Data breach concerns (69 percent)
- Supply chain disruptions (55 percent)

There is also no significant change in respondents' reporting of the type of threat actors behind exploits (**figure 34**). Cybercriminals (27 percent), hackers (20 percent), malicious insiders and nation-state actors (12 percent each) were still the top threat actors targeting enterprises. Notably, exploits attributed to nonmalicious insiders increased by three percentage points to 11 percent.

Social engineering remains the predominant cyberattack method and grew two percentage points (15 percent), followed by advanced persistent threat (APT) (11 percent), security misconfiguration (10 percent), ransomware (10 percent), unpatched system (10 percent), sensitive data exposure (9 percent) and denial of service (9 percent). A complete list of responses regarding attack types is shown in **figure 35**.

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

23 Eighty-one percent is the sum of "completely confident" responses (8 percent), "very confident" responses (34 percent) and "somewhat confident" responses (39 percent).

24 Eighty-one percent is the sum of the "strong positive impact" responses (36 percent) and the "some positive impact" responses (45 percent).

FIGURE 31: Organizational Confidence (2020-2023)

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

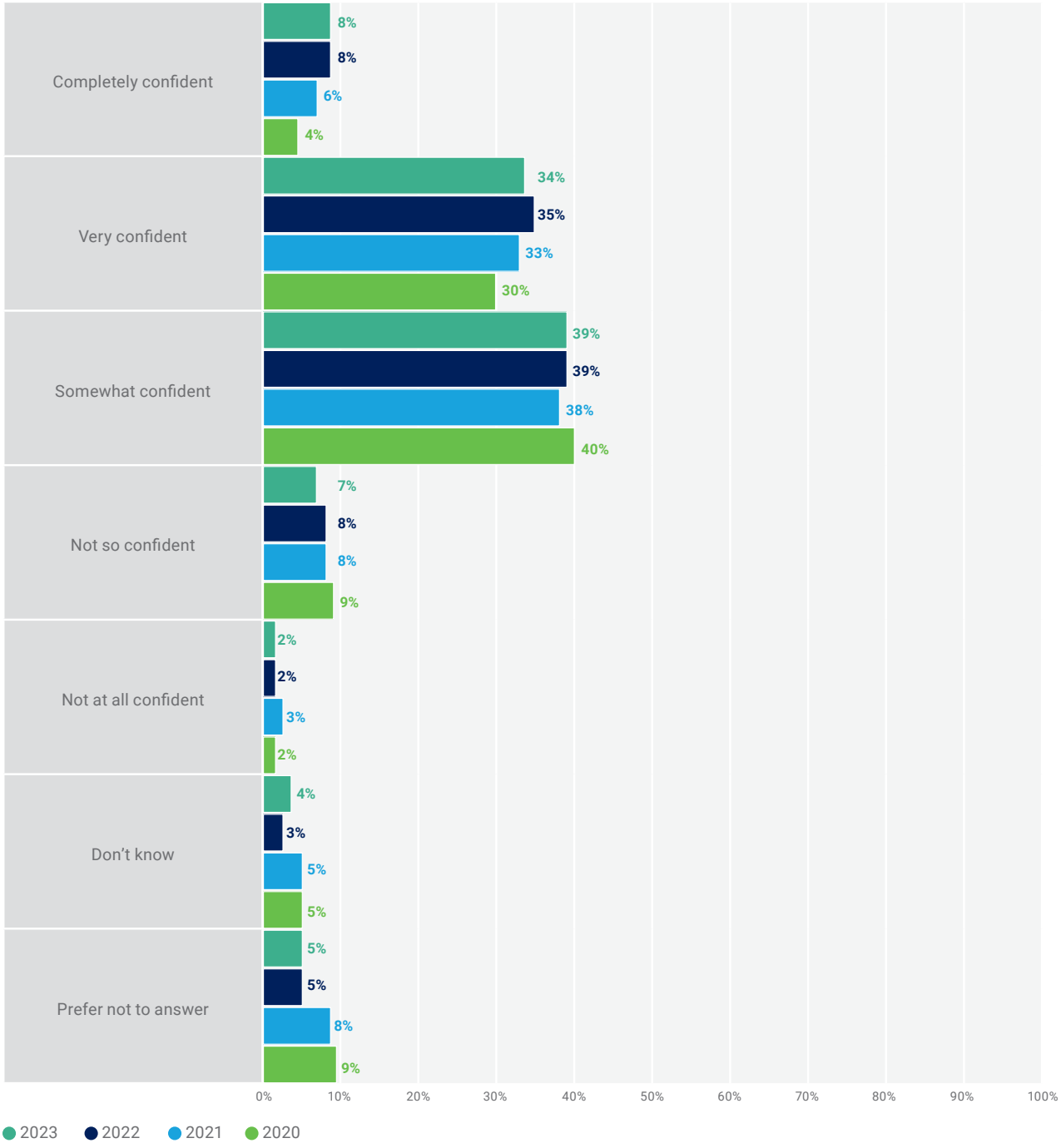


FIGURE 32: Cybersecurity Awareness Program Impact (2020-2023)

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

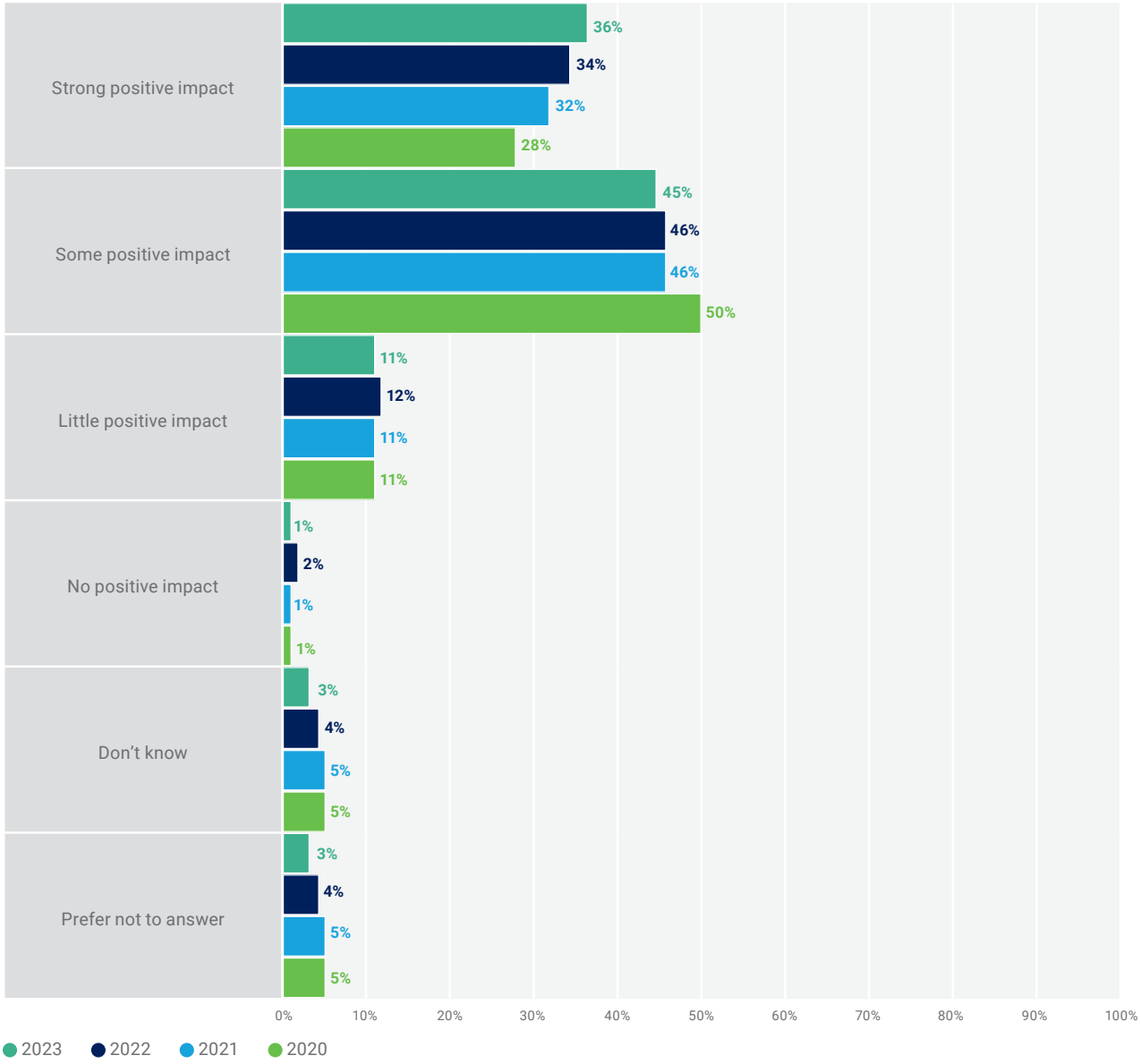


FIGURE 33: Organizational Cybersecurity Concerns

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

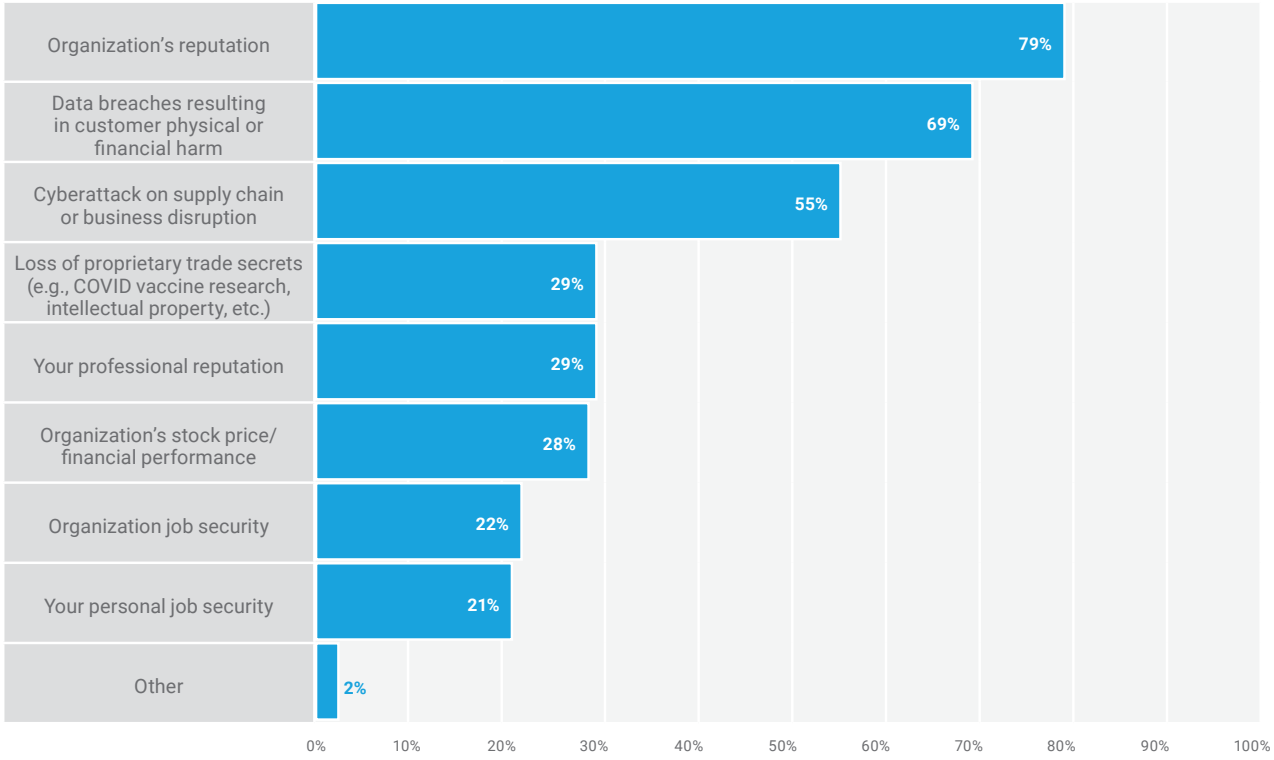


FIGURE 34: Threat Actors

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

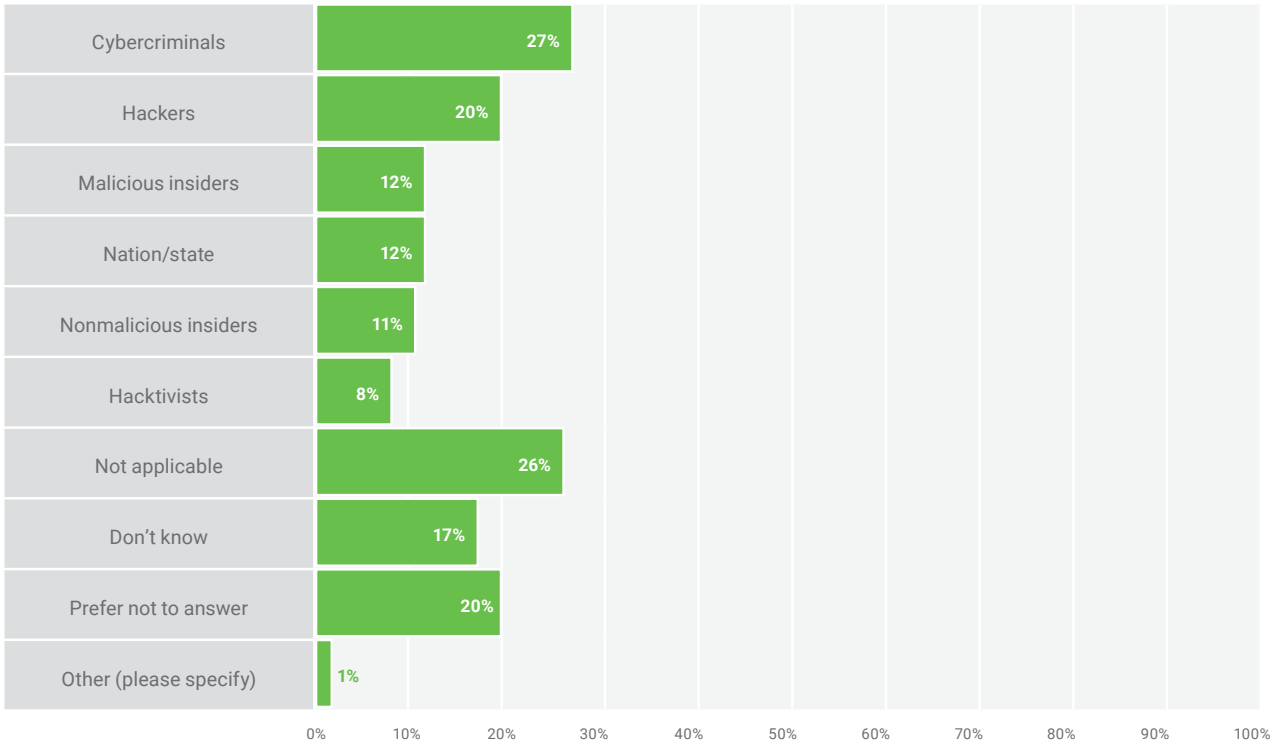


FIGURE 35: Attack Types

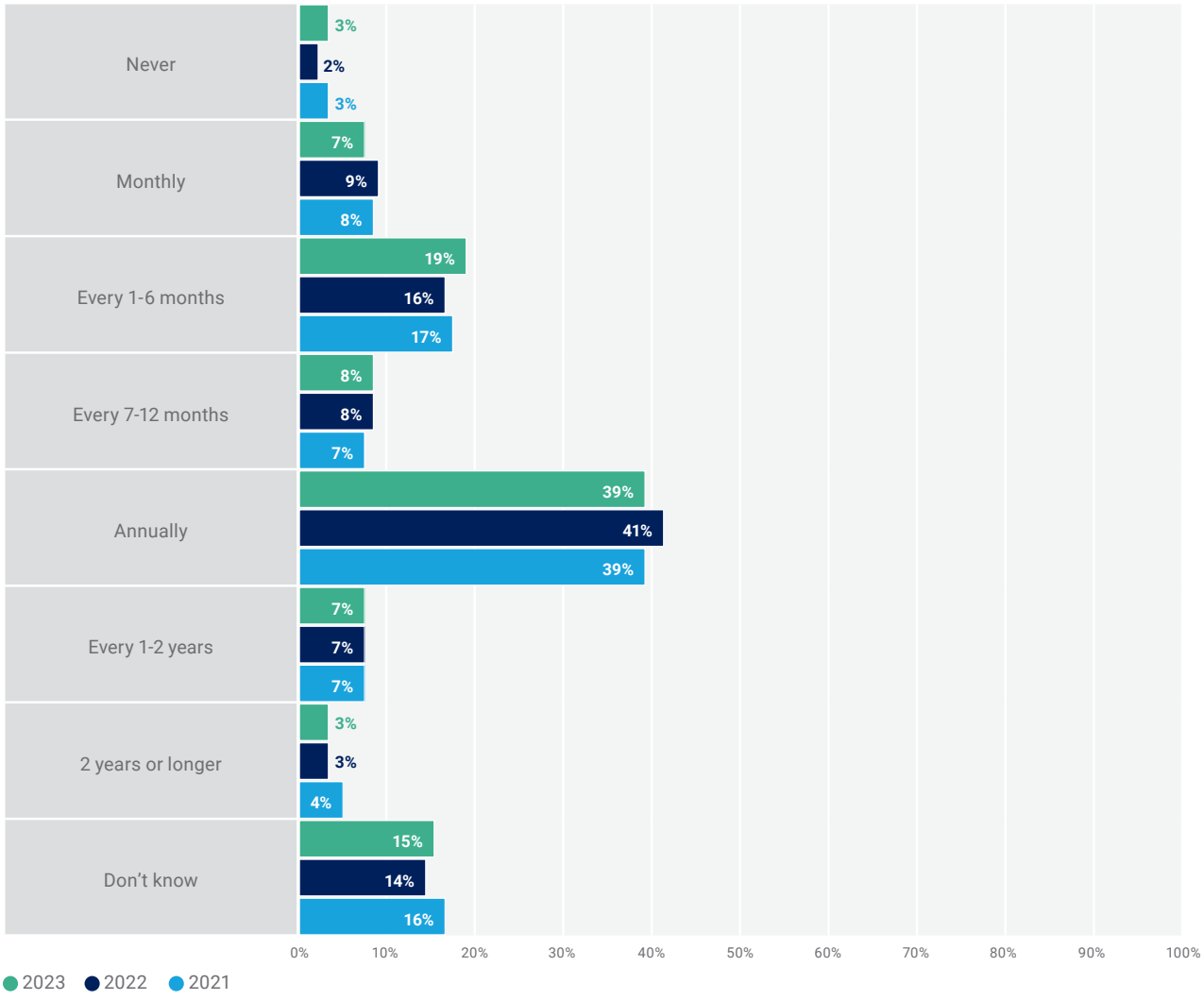
If your organization was compromised this year, which of the following attack types were used? Select all that apply.

Cybersecurity Maturity—A Work in Progress

ISACA carried over cybersecurity maturity questions into the 2023 survey to build upon the baseline data collection over recent years. Cybermaturity is generally understood as a correlation between readiness and organizational protective practices to prevent threats.[25] Little changed from 2022, with 55 percent of respondents stating their board of directors adequately prioritizes enterprise cybersecurity, while 75 percent believe their enterprise cybersecurity strategy is aligned with enterprise objectives. There were few shifts in the frequency of risk assessments from 2022 to 2023, but the three-percentage-point increase in those conducting assessments every one to six months (**figure 36**) is

FIGURE 36: Cyberrisk Assessment (2021-2023)

How often is a cyberrisk assessment performed on your organization?



25 ISACA, *Proactive Cybersecurity: A Quick Guide to Understanding Cyber Maturity*, USA, 2022, https://www.isaca.org/resources/proactive-cybersecurity-a-quick-guide-to-understanding-cyber-maturity

positive. Sixty-five percent of respondents' enterprises assess their cybermaturity, which nearly mirrors 2022 data (**figure 37**).

Conducting cyberrisk assessments remains a critical business activity for effectively monitoring risk factors and improving risk treatment options. The ranking of the barriers to conducting frequent cyberrisk assessments shifted from 2022. Time commitment was indicated as the primary barrier (41 percent), followed by a lack of personnel to perform assessments (38 percent)—both saw two-percentage-point declines from last year. A lack of cybertools increased by three percentage points, while the associated cost of cybertools increased by two percentage points. See **figure 38** for the year-over-year comparison of responses.

FIGURE 37: Cybermaturity Assessment

Does your organization currently assess its cybermaturity?

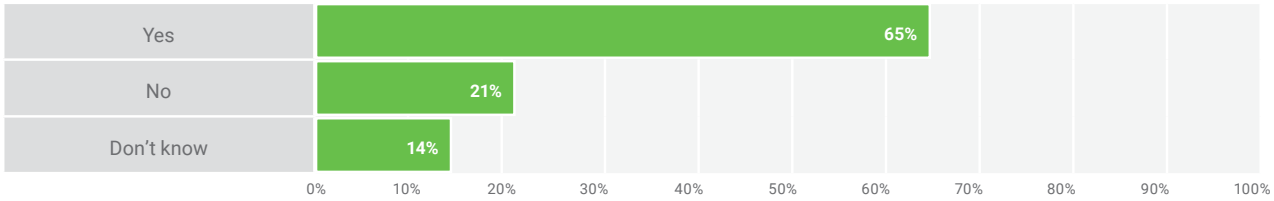
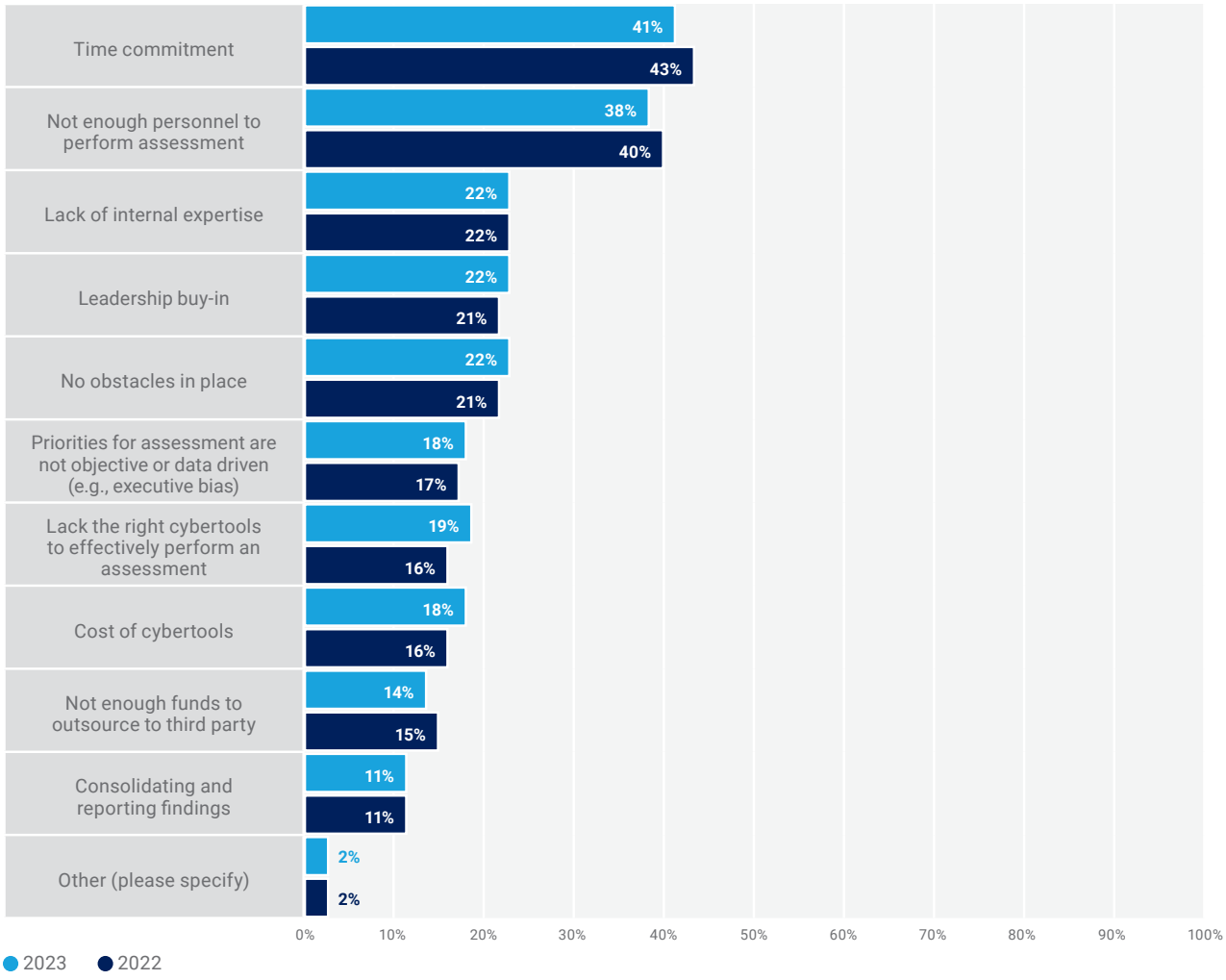


FIGURE 38: Cyberrisk Assessment Obstacles (2022–2023)

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



Organizational Alignment

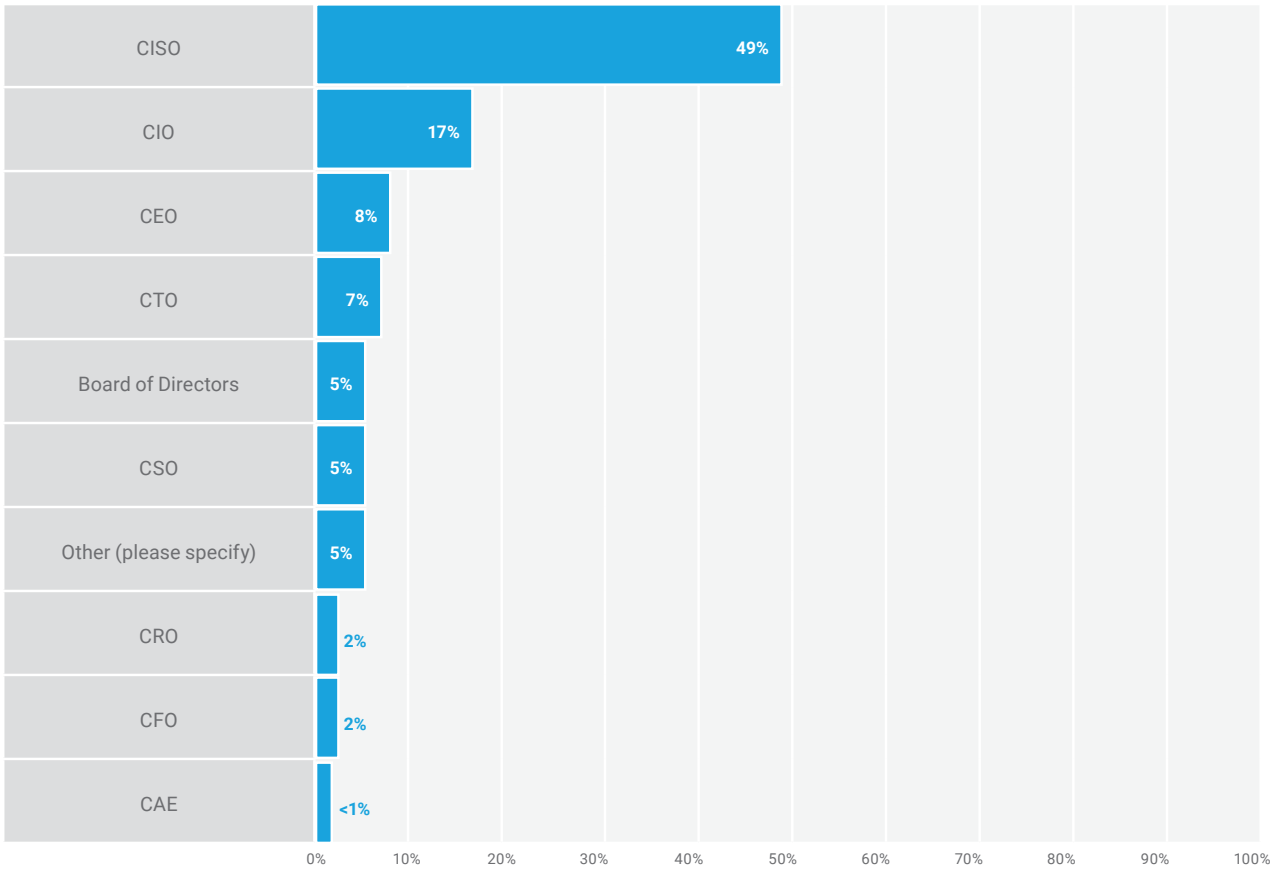
Nearly half of survey respondents reported that their enterprise cybersecurity team reports to a CISO (**figure 39**). However, whom the CISO reports to varies among two primary alignments—25 percent of respondents state their CISO reports to the CIO and 24 percent state they report to the CEO (**figure 40**).

While the role of CISOs has increased in scope, their position within an organization is far from uniform across enterprises; there is a prevailing belief that CISOs, let alone cybersecurity teams, should not report to any IT leader (e.g., CIO, CTO). Forrester research on this matter explored CISO alignment to CEOs, IT leaders and risk leaders (e.g., CFOs, CROs) and concluded based on evidence that CISOs aligned to CEOs have greater control and responsibility; experience less resistance, less reliance on third-party endpoint security products and fewer breaches; and enjoy greater organizational awareness of cybersecurity-related responsibilities.[26]

ISACA explored aspects of this issue, and respondent data show no significant correlation between enterprises who experienced more cyberattacks and who their cybersecurity team reported to, let alone whether the CISO reported to an IT leader versus others.

FIGURE 39: Cybersecurity Organizational Alignment

To whom does the cybersecurity team report in your organization?



26 Pollard, J.; "Five Reasons Why CISOs Should Report to CEOs," Forrester, 21 February 2023, https://www.forrester.com/blogs/five-reasons-why-cisos-should-report-to-ceos

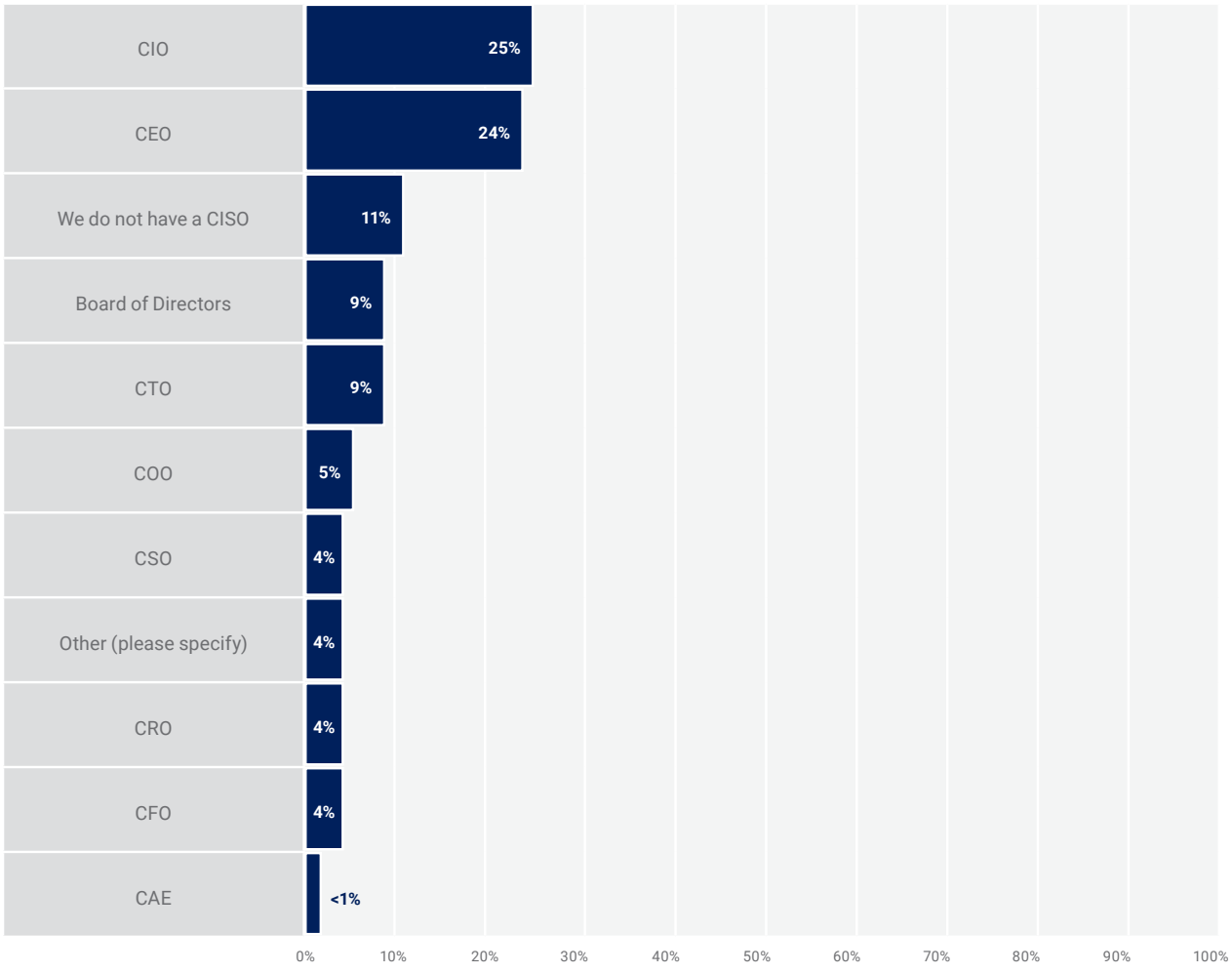
Those who indicated their organization's cybersecurity strategy is aligned with organizational objectives are significantly more likely to report to a CISO.

When not aligned, cybersecurity teams reporting is split between CISOs and CIOs.

Similarly, cybersecurity teams in organizations where the board of directors prioritizes cybersecurity are more likely to report to a CISO. Lack of board prioritization results in cybersecurity teams being split between reporting to a CISO or CIO. Those who reported no alignment are more likely to report to the CIO but twice as likely to not have a CISO or CSO.

FIGURE 40: CISO Organizational Alignment

To whom does the CISO report in your organization?



Conclusion—Little Has Changed

While the threat landscape is rapidly evolving, for most on the front lines, little has changed in recent years—a point reinforced by the longitudinal data from ISACA's *State of Cybersecurity* surveys. The cybersecurity workforce shortage is here to stay, and the existing workforce is aging. Anecdotal evidence suggests pathway programs into cybersecurity (e.g., reskilling, universities, apprenticeships) are creating sufficient output to minimally slow the divide between cybersecurity supply and demand. Industry reporting paints a different picture of increasing demand with little to no acknowledgment of pipeline supply initiatives, some of which are longstanding.

Return-to-office work mandates are ramping up despite job seekers' desire for remote work. Talks of a potential global recession appear to be taking a toll on signing bonuses and tuition reimbursement. With a low supply of cybersecurity talent, any further erosion—coupled with outmoded views on remote work—will surely hinder enterprises from filling open positions.

Cybersecurity budgets continue to level out with slight variations every other year. Views on budget planning are somewhat bleak, with a general belief that next year budgets will decrease.

Formal education continues to find itself in the crosshairs, and while there have been some minor improvements in technical areas, soft skills continue to be a growing area of concern. ISACA and others advocate for the removal of degree mandates, especially for entry-level positions. Experience repeatedly trumps any other qualification criterion. Increasing the talent pool should be of the utmost importance to hiring managers, which necessitates the creation of enough entry-level positions so that those who complete a cybersecurity pathway program can gain employment experience.

Cyberattack experience reporting saw little change, and the top enterprise concerns surrounding attacks include reputational damage, data breach concerns and supply chain disruptions.

Half of survey respondents employ a CISO, with the cybersecurity team reporting to this individual. CISOs predominantly report to a CEO or CIO. While data show this does not affect the likelihood and frequency of cyberattacks, there are connections between the board of directors' prioritization of cybersecurity and organizational alignment to business objectives.

Acknowledgments

ISACA would like to recognize:

Board of Directors

John De Santis, Chair

Former Chairman and Chief Executive Officer, HyTrust, Inc., USA

Brennan P. Baybeck, Vice-Chair

CISA, CISM, CRISC, CISSP

Senior Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

Stephen Gilfus

Managing Director, Oversight Ventures LLC, Chairman, Gilfus Education Group and Founder, Blackboard Inc., USA

Niel Harper

CISA, CRISC, CDPSE, CISSP, NACD.DC

Chief Information Security Officer, Data Privacy Officer, Doodle GmbH, France

Gabriela Hernandez-Cardoso

NACD.DC

Independent Board Member, Mexico

Jason Lau

CISA, CISM, CGEIT, CRISC, CDPSE, CIPM, CIPP/E, CIPT, CISSP, FIP, HCISPP

Chief Information Security Officer, Crypto.com, Singapore

Massimo Migliuolo

Independent Director, Former Chief Executive Officer and Executive Director, VADS Berhad Telekom, Malaysia

Maureen O'Connell

NACD.DC

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

Erik Prusch

Chief Executive Officer, ISACA, USA

Asaf Weisberg

CISA, CISM, CGEIT, CRISC, CDPSE, CSX-P

Chief Executive Officer, introSight Ltd., Israel

Pamela Nigro

ISACA Board Chair 2022-2023

CISA, CGEIT, CRISC, CDPSE, CRMA

Vice President, Security, Medecision, USA

Gregory Touhill

ISACA Board Chair 2021-2022

CISM, CISSP

Director, CERT Center, Carnegie Mellon University, USA

Tracey Dedrick

ISACA Board Chair, 2020-2021

Former Chief Risk Officer, Hudson City Bancorp, 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 Adobe

Adobe is changing the world through digital experiences. Great experiences have the power to inspire, transform and move the world forward. And every great experience starts with creativity. Creativity is in Adobe's DNA and the future belongs to those who create. Adobe's game-changing innovations are redefining the possibilities of digital experiences. Adobe connects content and data and introduces new technologies that democratize creativity, shape the next generation of storytelling and inspire entirely new categories of business. Adobe is committed to protecting the security, privacy and availability of its products, systems and data—so partners can deliver trusted experiences every day.

Website: https://trust.adobe.com

Contact: trustcenterquestions@adobe.com

DISCLAIMER

ISACA has designed and created *State of Cybersecurity 2023: 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.

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

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/

Adobe

Dive deeper with our Security@Adobe newsletter

Learn security best practices from our experts and keep up with our latest innovations. Six times a year, delivered right to your inbox.