ISACA Adobe

State of Cybersecurity 2024

Global Update on Workforce Efforts, Resources, and Cyberoperations

Information Security

CONTENTS

ABSTRACT

State of Cybersecurity 2024: 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 2024. This survey report focuses on the current trends in cybersecurity workforce development, staffing, and budgets; threat landscape; cyberrisk; and use of artificial intelligence (AI). Although past annual cybersecurity reporting did not indicate major shifts in views or trends, 2024 survey data reveal multiple changes which carry the potential to adversely affect cybersecurity readiness.

Executive Summary

The tenth annual ISACA® global *State of Cybersecurity Survey* continues to identify current challenges and trends within the cybersecurity field, while ISACA continues to expand its longitudinal reporting with year-over-year comparison survey results in *State of Cybersecurity 2024*. This year's report analyzes survey results on cybersecurity skills, staffing, and budgets; cyberthreats; cyberrisk; and, new this year, artificial intelligence (AI).

Compared with prior year, some survey-result data has not changed, while other data reinforce the finding last year that market uncertainty is having a marked impact—especially on budgets and compensation, which carry the potential to adversely affect cybersecurity readiness.

Key findings include:

- The aging workforce is growing. For the first time in the 10 years of this survey, the largest percentage of respondents are between the ages of 45 and 54 (34 percent). This age group overtakes respondents between the ages of 35 and 44 (30 percent). These results, combined with no uptick in the percentage of respondents who are ages 34 and below and no increase in the number of respondents who manage staff with less than three years of experience, are an alert to industry leaders to consider succession plans for any sudden increase in attrition.
- This year's survey findings show a slight improvement in appropriate staffing levels. Thirty-eight percent of respondents believe that their cybersecurity team is appropriately staffed, which is an increase of two percentage points over last year's results. Respondents who believe that their team is somewhat understaffed (43 percent) decreases by three percentage points from last year. Analysis reveals no relationship between staffing levels and whether enterprises use AI to mitigate shortfalls.
- Sixty-six percent of respondents report that occupational stress is much higher than five years ago—81 percent of respondents attribute the higher stress to an increasingly complex threat environment.
- Open cybersecurity roles at all levels continue to wane. Survey data reveal steep declines in vacant technical and nontechnical individual-contributor positions. Cybersecurity manager positions drop nine percentage points (from 60 percent) to their lowest level ever reported for the *State of Cybersecurity Survey*. Senior manager/director vacancies decrease for the third consecutive year. Executive cybersecurity positions do the same, but not as severe.
- Economic conditions appear to be discouraging employees from leaving current jobs—especially within the United States. The top two reasons why cybersecurity professionals leave their jobs are selected by fewer respondents this year—recruitment by other companies drops by eight percentage points to 50 percent and poor financial incentives drops by four percentage points to 50 percent. High work-stress levels jumps to 46 percent—three percentage points higher than last year's survey results. The ongoing employer-employee struggle over return-to-office mandates is likely fueling the increase of four percentage points in respondents who identify limited remote work possibilities as a reason for attrition.

Economic conditions appear to be discouraging employees from leaving current jobs—especially within the United States.

- Employer benefits are shrinking. Fewer employers are paying for professional development training, dropping seven percentage points from last year's survey results. Employers offering flex hours shows a similar drop this year.

- Hands-on cybersecurity experience continues to be the primary factor in determining whether a candidate is considered qualified. Although views on credentials and hands-on training are unchanged, respondents place less emphasis on prior-employer recommendations and university degrees. Respondents report an increase in the importance of association membership.
- Leveraging training to allow interested nonsecurity professionals to move into security roles and increased use of contractors or consultants remain the primary mitigations for the cybersecurity technical skills gaps. Training decreases by four percentage points, and increased use of contractors or consultants increases by two percentage points. After last year's decline, increased reliance on AI or automation to address staffing shortages rebounds to 23 percent. The use of apprenticeship or internship programs decreased by three percentage points.
- Cybersecurity funding levels drop significantly this year, and its incremental year-over-year decline shows signs of a potential multiyear freefall. Just thirty-six percent of respondents indicate that their cybersecurity budgets are appropriately funded, and 44 percent of respondents believe that their budgets are somewhat underfunded—an increase of four percentage points. Only 47 percent of respondents believe that budgets will increase, and 41 percent of respondents report that budgets will plateau. Thirteen percent of respondents expect budgets to shrink over the next year—a view that is incrementally growing since 2022.
- Threat-landscape data change very little, with two caveats—exploitations attributed to nonmalicious insiders drops to 9 percent, which is an acceptable metric for effective insider-threat and cybersecurity education and awareness training programs. Respondents indicating the "Not applicable" answer declines five points, which is not surprising given an increasingly complex threat landscape.
- Almost half do not know what kind of cyberinsurance their enterprise carries. From a regional perspective, 57 percent of those in Oceania lacked knowledge of their enterprise cyberinsurance type, followed by North America (49 percent) and Europe (43 percent).
- Use of AI in security operations remains in its infancy. Threat detection/response (28 percent) and endpoint security (27 percent) are the most popular applications. Eighteen percent of respondents prefer to not answer. The number of respondents reporting that either they or a team member are involved in the development, onboarding, or implementation of AI solutions is disheartening. Nearly half (45 percent) report no involvement. Results are similar regarding respondent involvement in the development of AI governance policies.

Survey Methodology

In the second quarter of 2024, ISACA sent online survey invitations to a global population of cybersecurity professionals.

These professionals hold the ISACA Certified Information Security Manager® (CISM®) certification or have registered job titles in the information security field.

The survey uses multiple-choice and Likert-scale formats and presents respondents with questions across six focus areas:

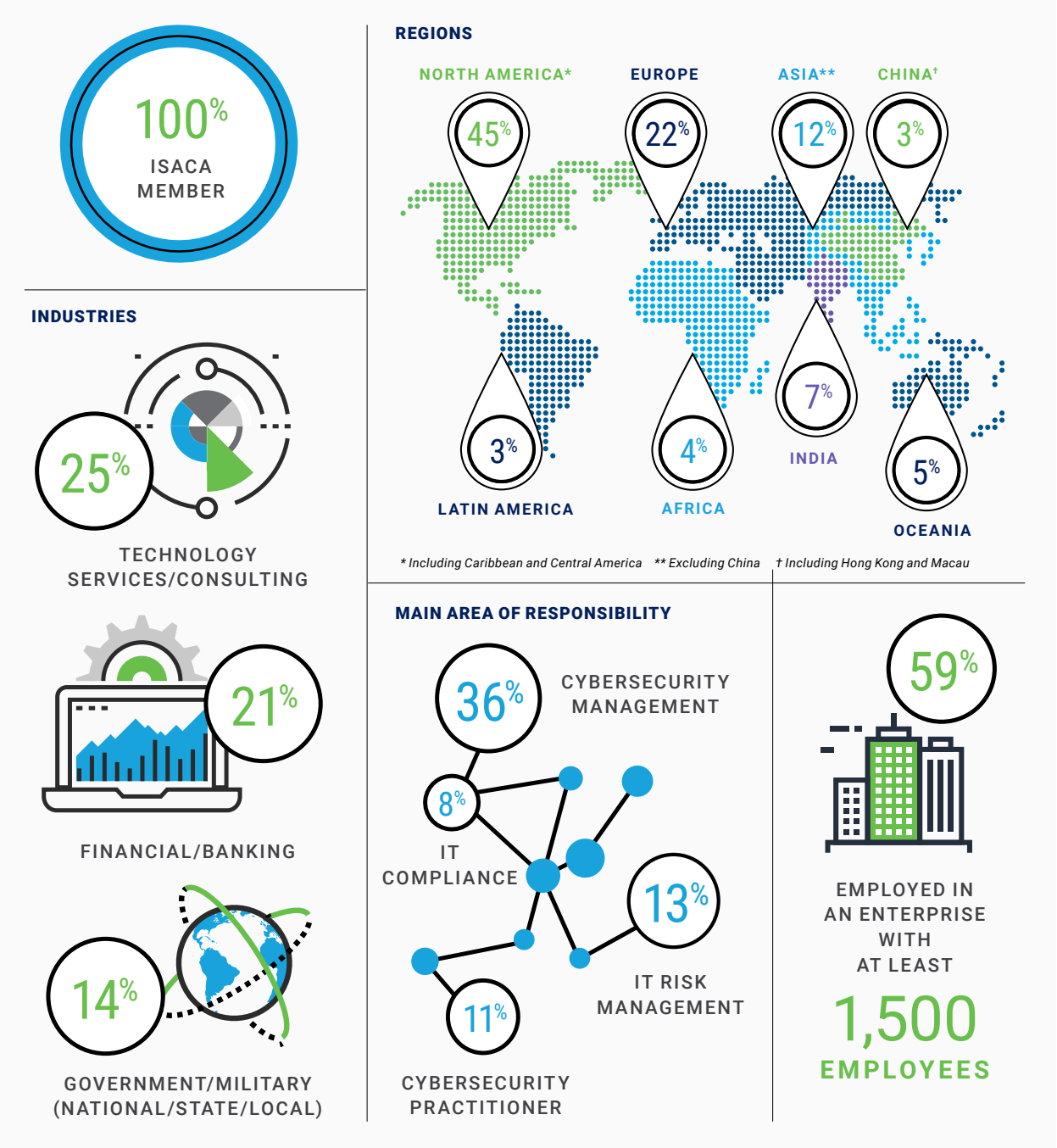
- Hiring and Skills
- Security Operations
- Cybersecurity budgets
- Cyberattacks and Cyberthreats
- Cyberrisk Assessments
- Organizational Cybersecurity and Governance

A total of 1,868 respondents completed the survey in its entirety, and their responses are included in the results.[1]

This survey has a margin of error of +/- 2 percent at a 95-percent confidence interval. Survey data was collected anonymously, and response rates vary by question.

Of the 1,868 respondents, 47 percent indicate that cybersecurity is their primary professional area of responsibility. **Figure 1** shows demographic information about the respondents, who hail from 102 countries and territories. **Figure 2** further illustrates the breadth of survey input, showing that respondents represent more than 17 industries.

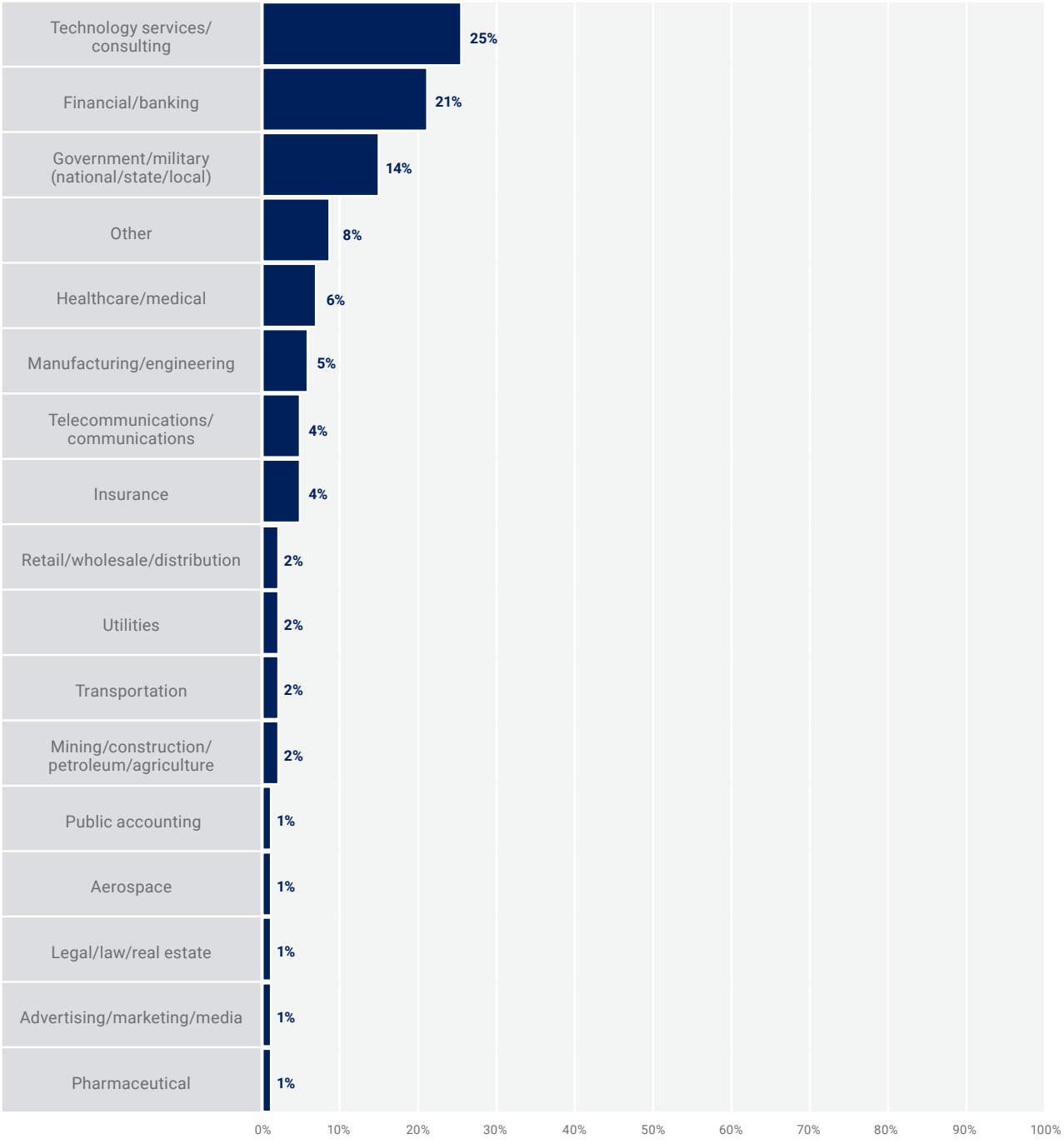
FIGURE 1: Respondent Demographics



1 Some survey 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 2: Industries Represented

Please indicate your organization's primary industry.



Cybersecurity Workforce Challenges

Staffing

The percentage of ISACA survey respondents who manage security staff with less than three years of work experience is unchanged (44 percent) for a third consecutive year. Meanwhile, the 2023 spotlight on an aging workforce is trending worse. This year, the age group of respondents between the ages of 45 and 54 (34 percent) overtakes the 35-to-44 age group (30 percent). The percentage of respondents who are ages 34 and below is showing no improvement (**figure 3**).

Respondents report a slight improvement in appropriate staffing (**figure 4**). Thirty-eight percent of respondents believe that their cybersecurity team is appropriately staffed, which is two percentage points higher than last year. Respondents who report that their cybersecurity team is somewhat understaffed decreased three percentage points from 2023. Further analysis shows no correlation between staffing levels and whether enterprises use AI to mitigate shortfalls.

FIGURE 3: Workforce by Age

Please select your age.

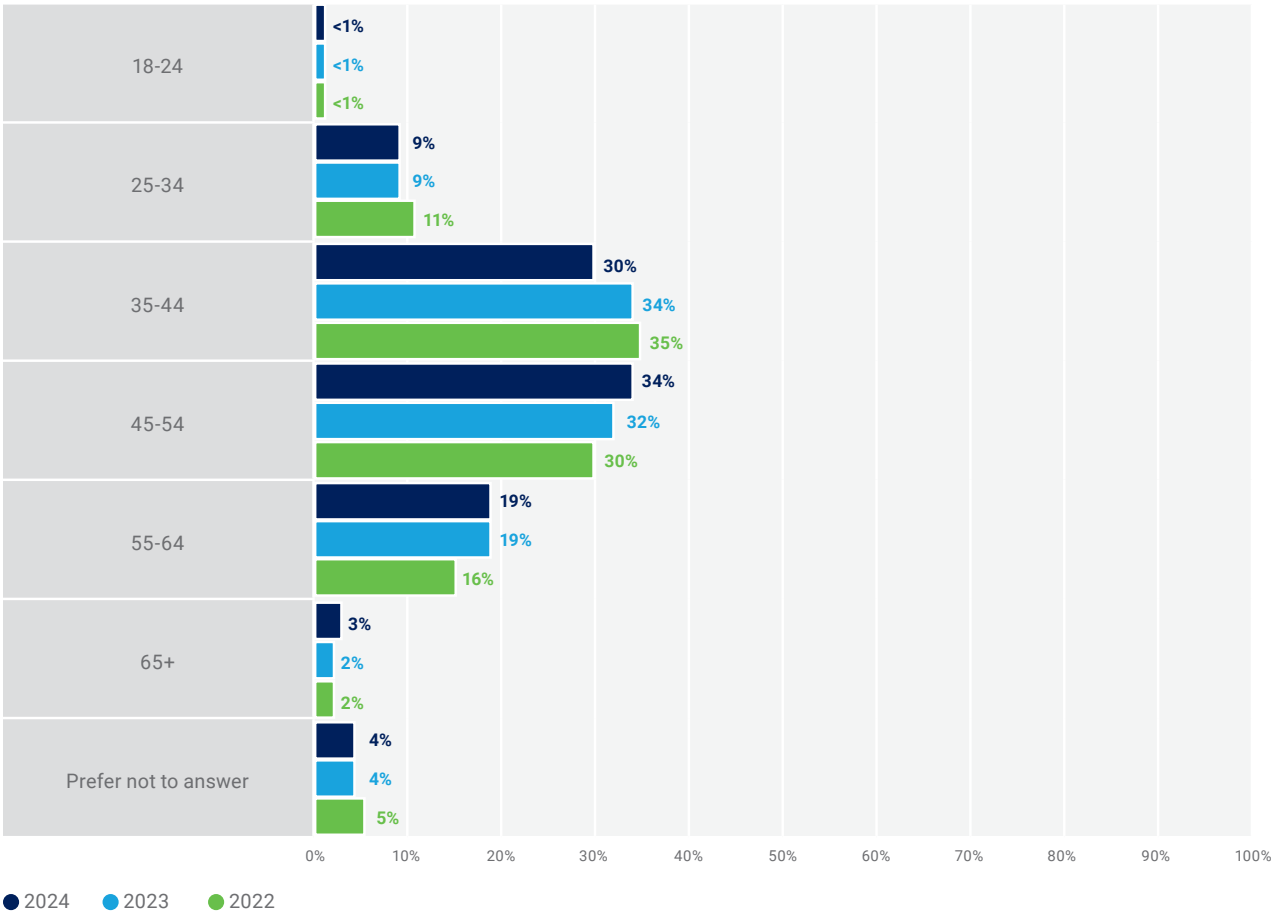
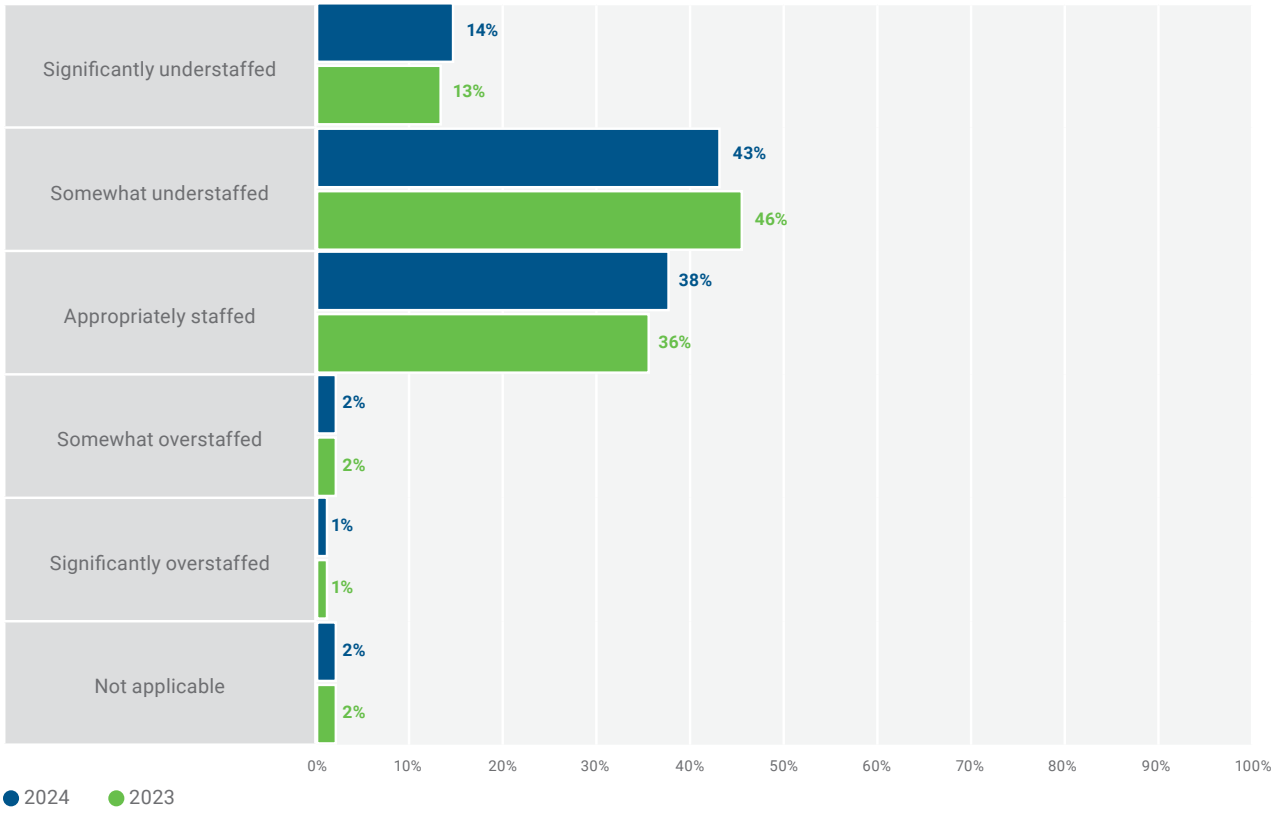


FIGURE 4: Cybersecurity Staffing

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



Retention

Retention remains level relative to last year's results and represents a notable shift in employee behavior[2] from the Great Resignation to the Big Stay—many believe this pattern reflects broad economic uncertainty and the geopolitical landscape.[3] Regional data reveals marked differences across reporting areas, with North America reporting the least difficulty retaining talent (**figure 5**). Regardless of individual reasons to remain in place or pursue new opportunities, respondent data affirms the trend observed previously in ISACA survey results that uncertainty of any kind is usually accompanied by better retention (**figure 6**).

Sixty-six percent of respondents indicate that their level of occupational stress is higher now than it was five years ago. When asked why their role is more stressful, 81 percent of respondents attribute the increase to an increasingly complex threat environment (**figure 7**).

2 Kalser, A.; "Employees are staying put — but how long will that last?," HR DIVE, 23 May 2024, www.hrdive.com/news/attrition-low-but-for-how-long/716827/

3 PoliteMail, "How the Big Stay Has Replaced the Great Resignation," 13 March 2024, https://politemail.com/how-the-big-stay-has-replaced-the-great-resignation/

FIGURE 5: Retention Difficulty by Region[4]

Has your organization experienced difficulties retaining qualified cybersecurity professionals?

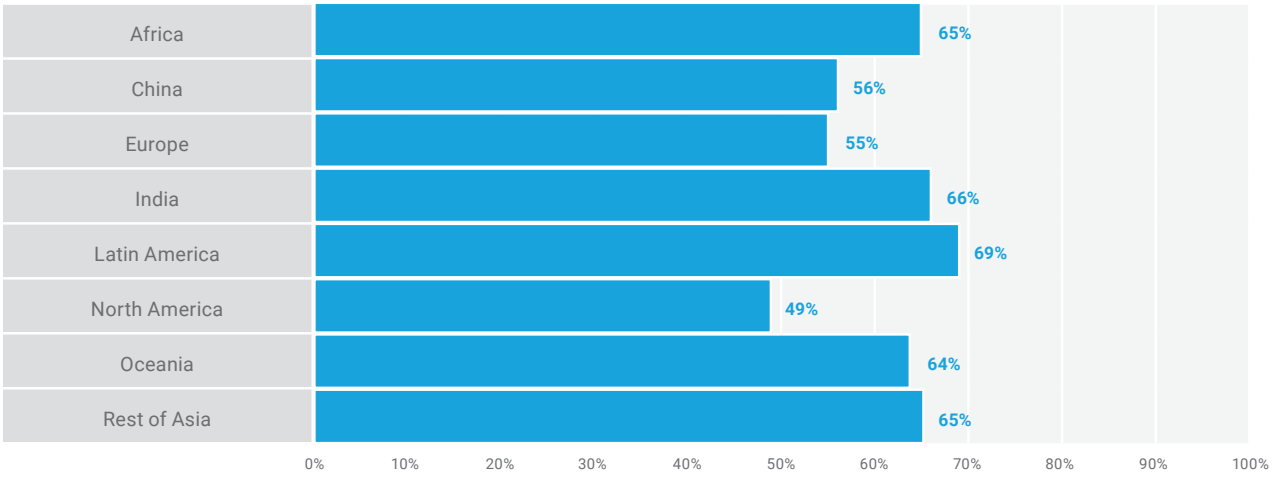
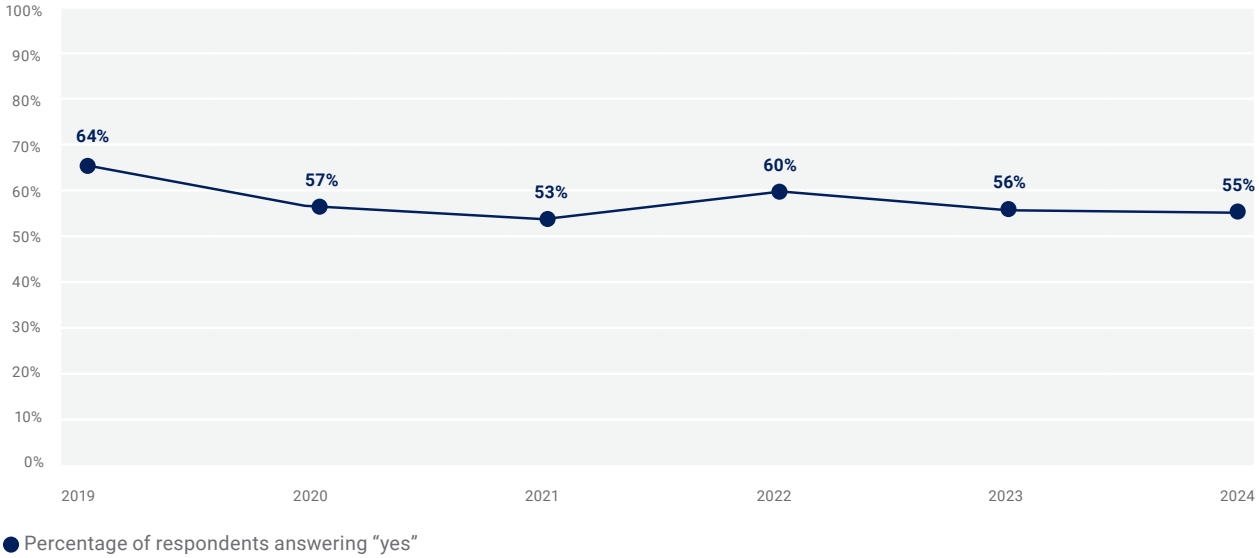


FIGURE 6: Retention Difficulties (2019-2024)[5]

Has your organization experienced difficulties retaining qualified cybersecurity professionals?

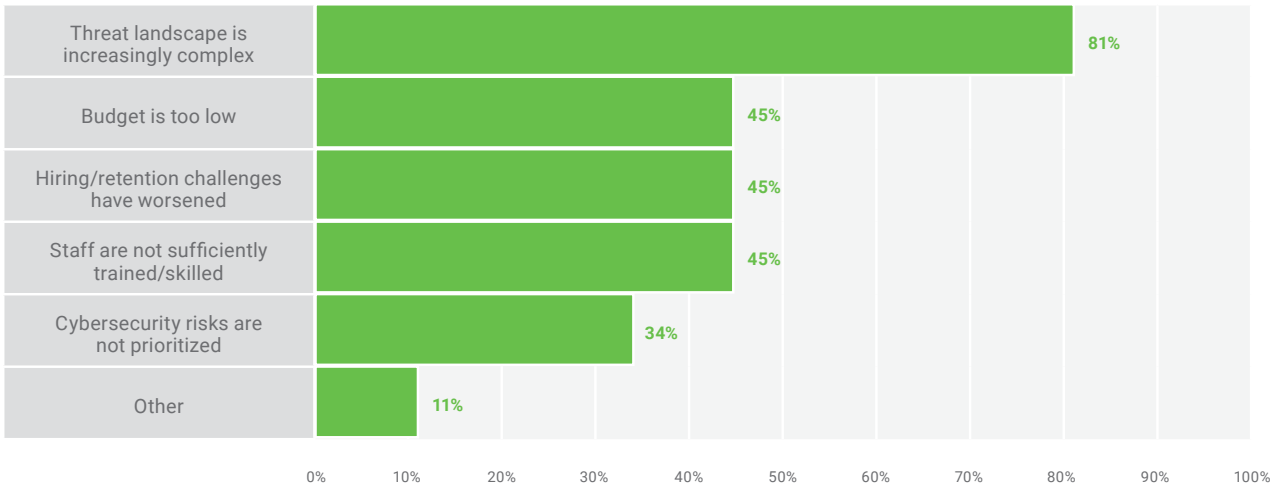


4 The figure depicts the percentage of "Yes" responses to the question by reporting region.

5 The figure depicts "Yes" responses for the years 2019 to 2024.

FIGURE 7: Sources of Stress

Please tell us why your role is more stressful today than it was 5 years ago.



Vacancies

Forty-six percent of survey respondents report that their enterprise has open non-entry-level cybersecurity positions, which is down four percentage points from last year.

Eighteen percent of respondent enterprises have open entry-level positions, which is a three percentage-point drop from 2023 (**figure 8**). Also of interest, the percentage of respondents who report no open positions increases three percentage points over last year.

Time to Fill Open Positions

Respondents report almost no differences in the times to fill entry-level and non-entry-level positions from the times reported in 2023. The lone change is a slight increase of two percentage points in non-entry-level positions reportedly taking three-to-six months to fill (38 percent in 2023) (**figure 9**).

FIGURE 8: Unfilled Positions

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

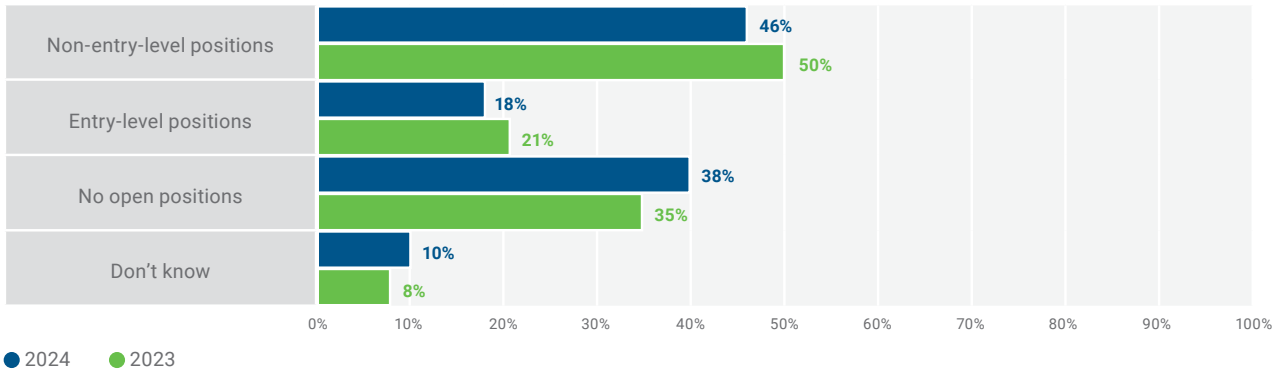
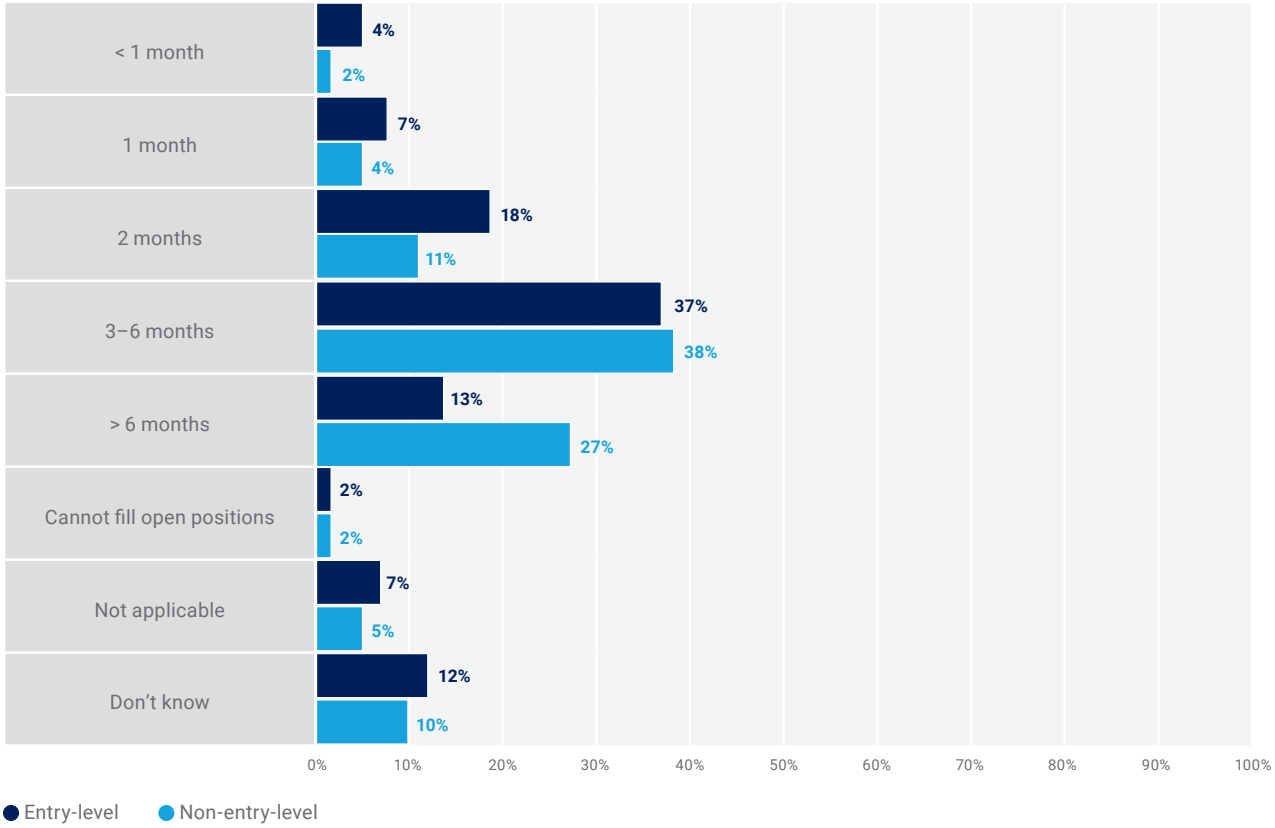


FIGURE 9: Time to Fill Cybersecurity Positions

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



Analyzing Unfilled Positions

Technical nonsupervisory cybersecurity positions remain the top category of vacancies (**figure 10**), but the real story this year can be seen in the longitudinal data for individual contributors and management levels in **figure 11** and **figure 12**, respectively. Survey data reveal steep declines in vacant technical and nontechnical individual-contributor positions—13 and 9 percentage points, respectively. Cybersecurity manager positions drop nine percentage points (from 60 percent) to the lowest level reported for the *State of Cybersecurity Survey*. Senior manager/director-level vacancies declined for the third consecutive year to 40 percent. Executive cybersecurity positions also declined—but nominally to 28 percent (from 31 percent).

Survey data reveal steep declines in vacant technical and nontechnical individual-contributor positions. Cybersecurity manager positions drop nine percentage points to the lowest level reported for the *State of Cybersecurity Survey*.

Future Demand

Demand for technical individual contributors has remained high for many years, and, although future demand for this position is still high, it declined last year and continues to fall (by five percentage points) to the lowest level reported for the *State of Cybersecurity Survey* (**figure 13**).

FIGURE 10: Percentages of Unfilled Positions at Given Organizational Levels

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

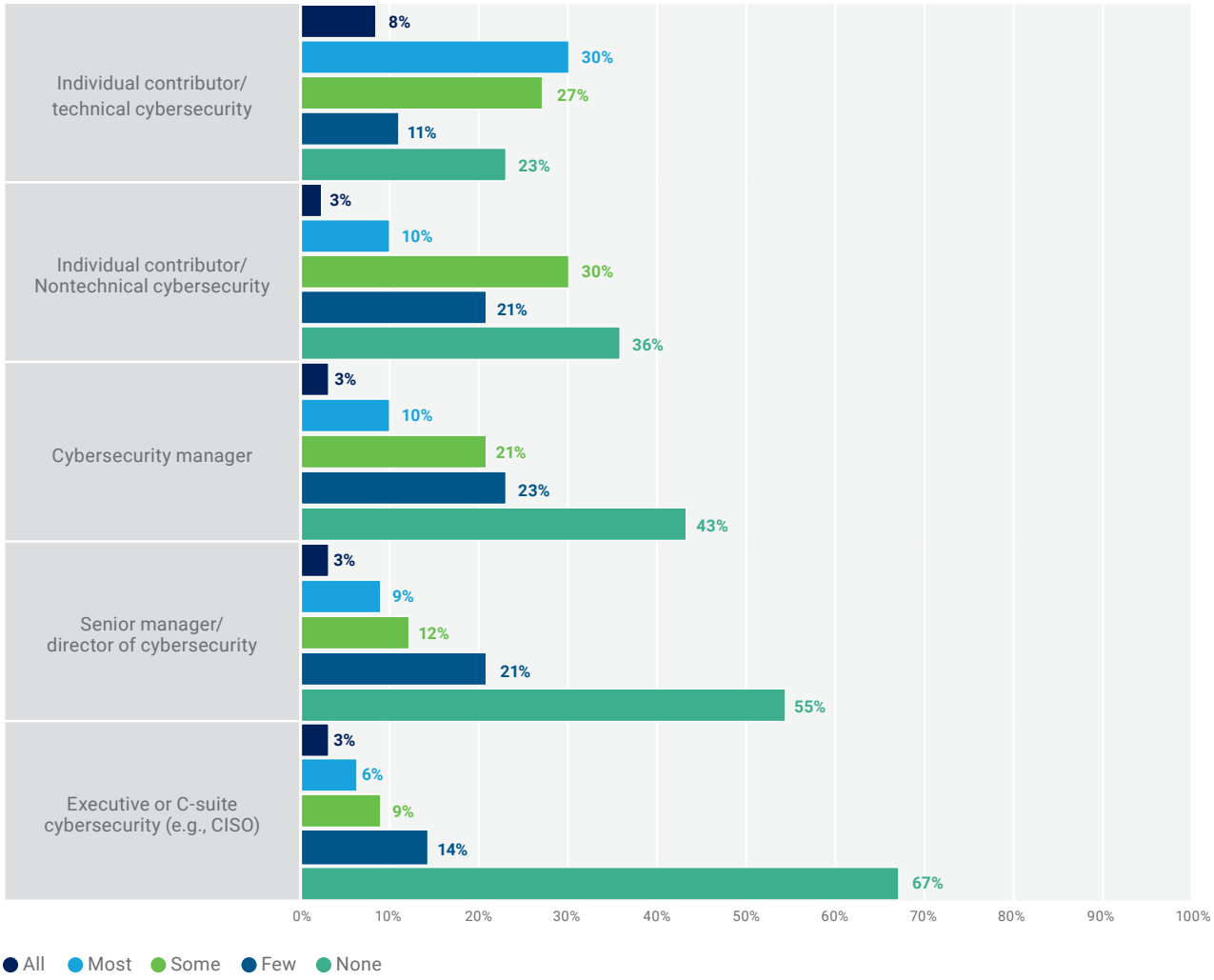
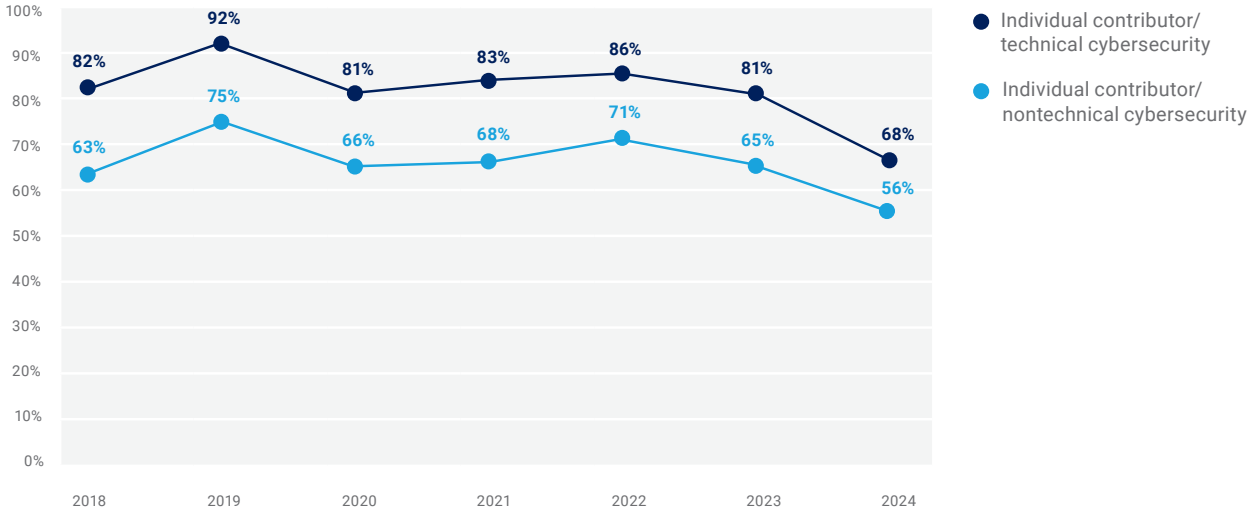


FIGURE 11: Unfilled Positions Reporting—Individual Contributors (2018-2024)[6]



6 This figure compares reported unfilled position data from 2018 to 2024 survey results. Percentages represent the sum of all reported vacancy percentages for each position and exclude the "Don't Know" and "None" responses.

FIGURE 12: Unfilled Position Reporting—Management (2018-2024)[7]

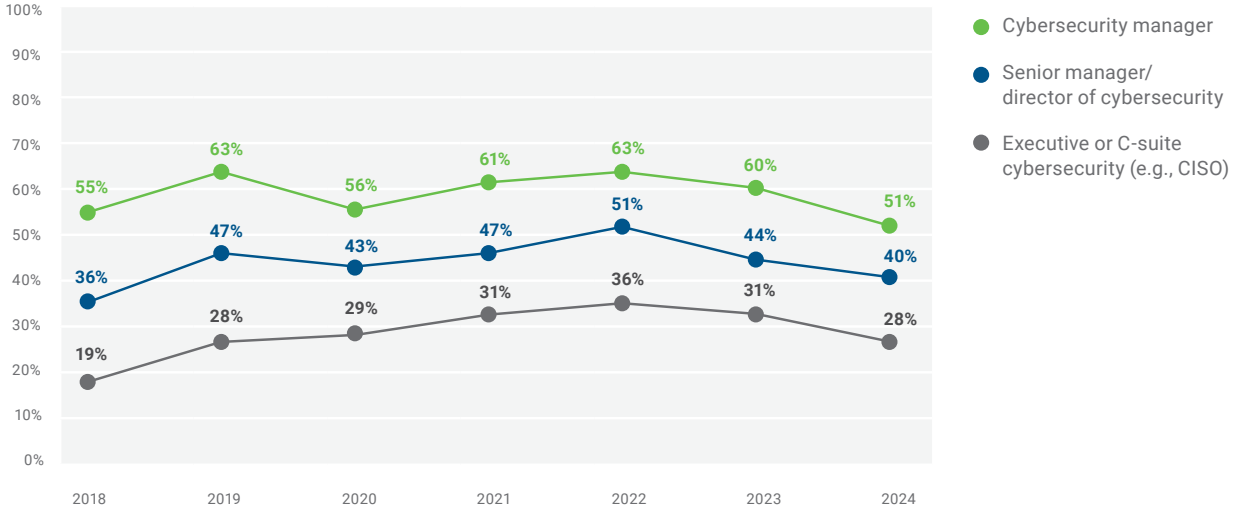
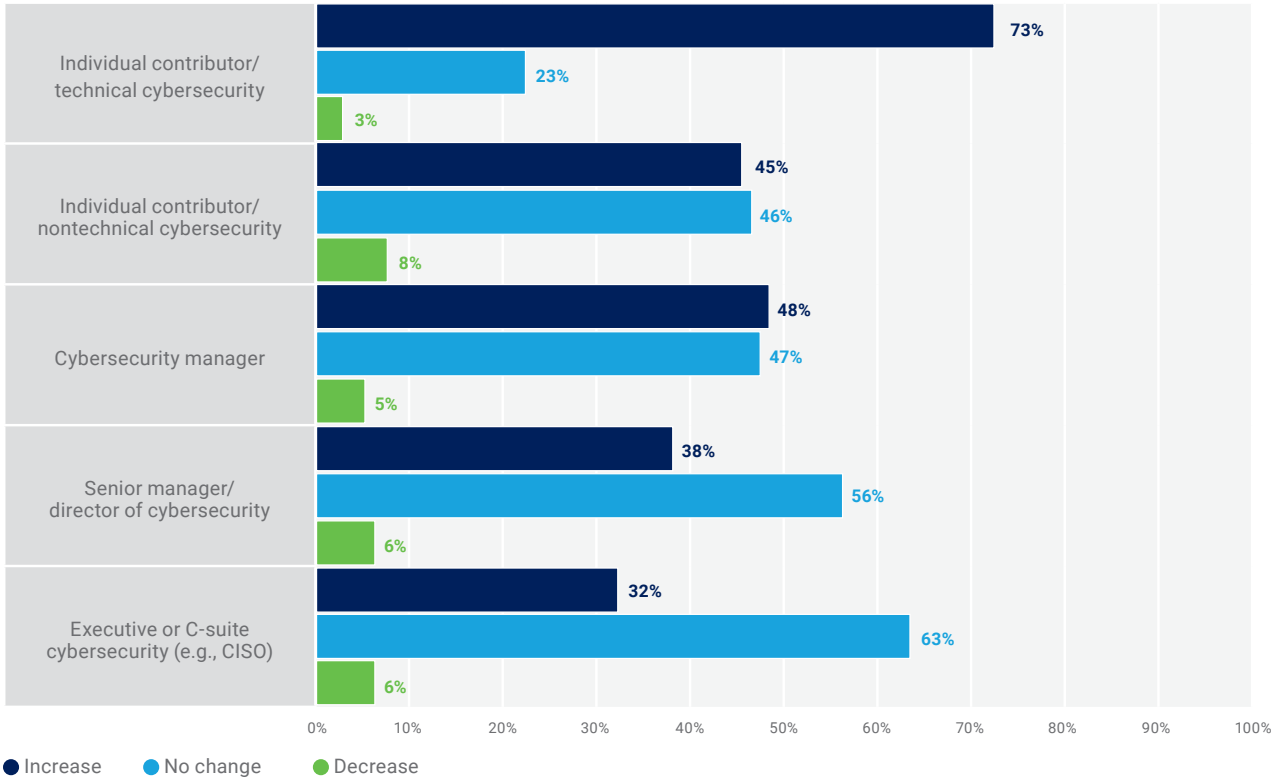


FIGURE 13: Future Hiring Demand

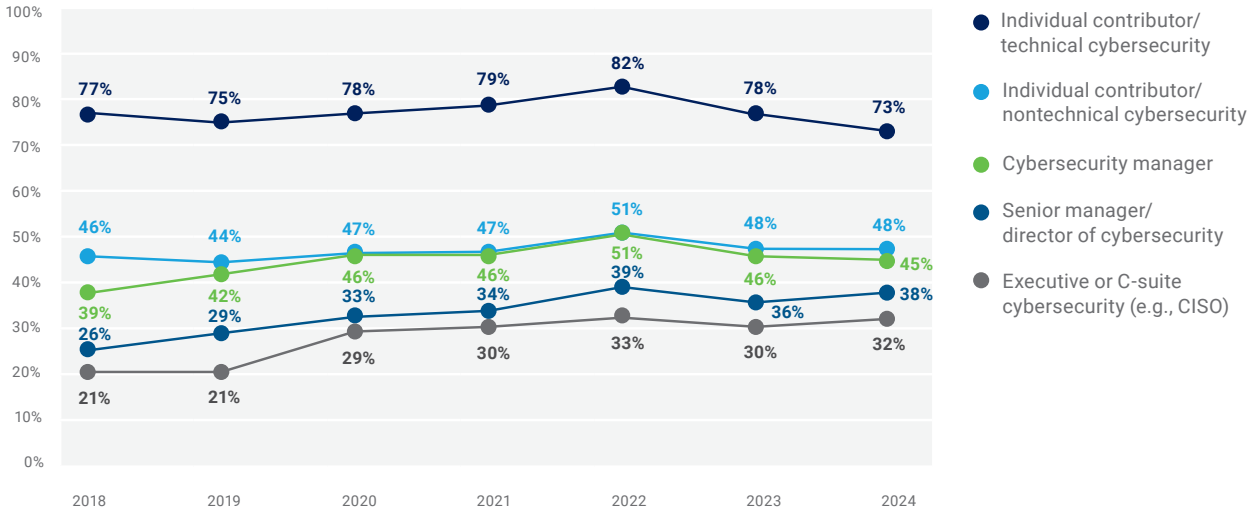
In the next year, do you see the demand for the following cybersecurity position levels increasing, decreasing, or remaining the same?



7 This figure compares reported unfilled position data from 2018 to 2024 survey results. Percentages represent the sum of all reported vacancy percentages for each position and exclude the "Don't Know" and "None" responses.

Future demand for nontechnical individual contributor and cybersecurity manager positions are unchanged, while future demand for senior- and executive-level cybersecurity positions is reported to increase slightly, each increasing two percentage points from the previous year. Note that the seven-year trend between years is very similar for technical and nontechnical individual contributors. **Figure 14** shows historical views on this question.

FIGURE 14: Hiring Demand Trending (2018-2024)



Attrition

As previously stated, industry reporting suggests that economic conditions are discouraging employees from leaving current jobs—at least within the United States. However, attrition cannot be entirely prevented. Although the cybersecurity profession historically favors well-qualified job seekers, this year's data reflects large drops in the top two reasons why cybersecurity professionals leave their jobs (**figure 15**). Recruitment by other companies and poor financial incentives remain the largest perceived reasons why cybersecurity professionals leave positions—each at 50 percent. High work-stress levels increase by 3 percentage points (46 percent), which is a rebound from last year's minor dip. High work stress is now tied with limited promotion and development opportunities, which decreases 2 percentage points from one year ago. The ongoing employer-employee struggle over return-to-office mandates is likely fueling the increase in the percentage of respondents who believe that limited remote work possibilities is a cause for cybersecurity professionals leaving their current jobs, which rose four percentage points from 2023 and eight percentage points since 2022.

Employer Benefits Are Decreasing

The 2024 survey data show that employer benefits are tightening (**figure 16**). Respondents report major cuts to professional development training (seven percentage-point drop) and a six percentage-point fall in employers offering flex hours. Professional development budgets are commonly cut when enterprises seek cost savings. The reasons for cutting this budget are not conclusive but may include unclear business value.[8] The favorable reporting on employer benefits is that employers are still covering employee certification fees, and university tuition reimbursement increases slightly.

8 Everett, C.; "Training budgets first to be cut due to unclear business value," HR Zone Ltd, 14 February 2012, https://hrzone.com/training-budgets-first-to-be-cut-due-to-unclear-business-value/

FIGURE 15: 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?

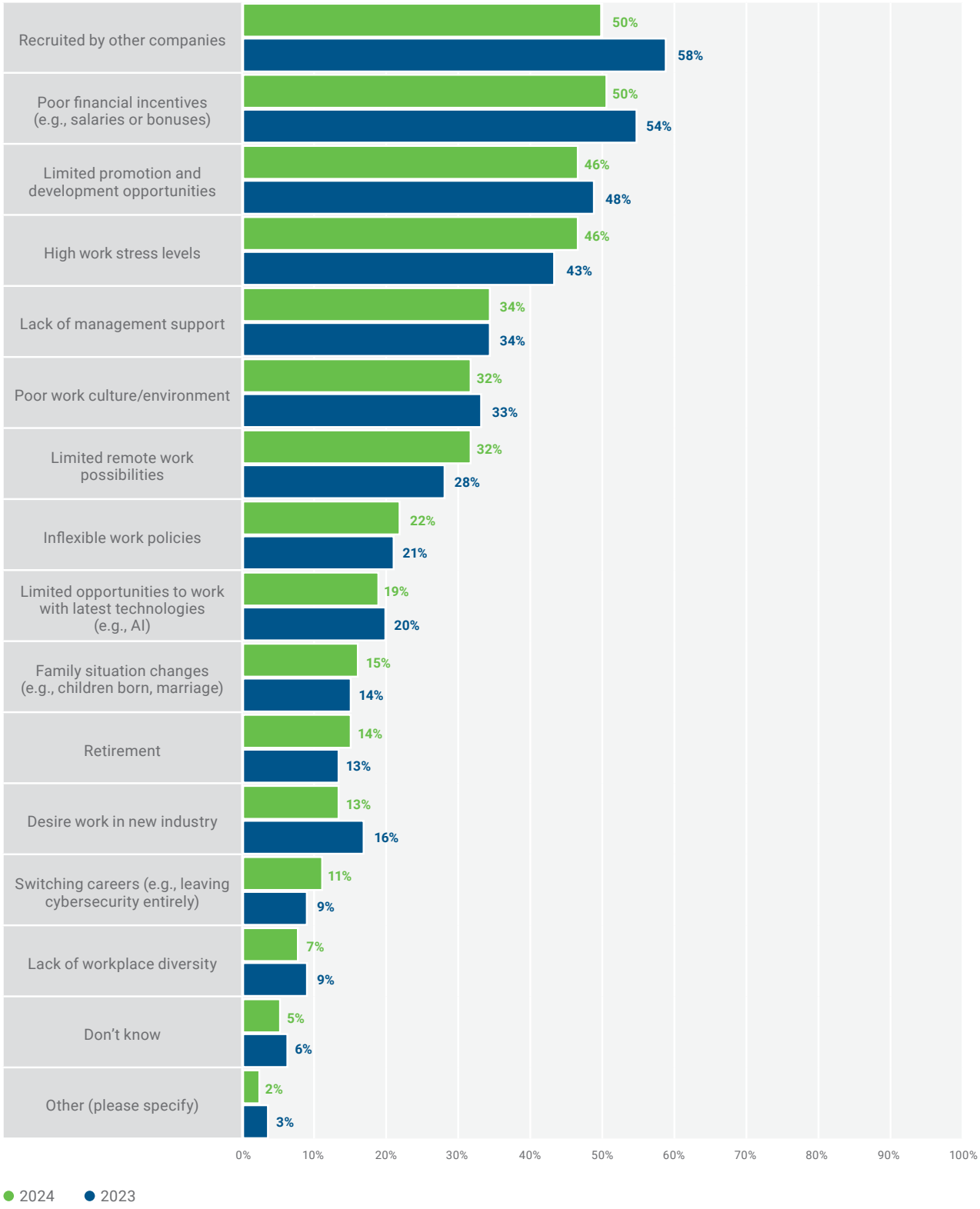
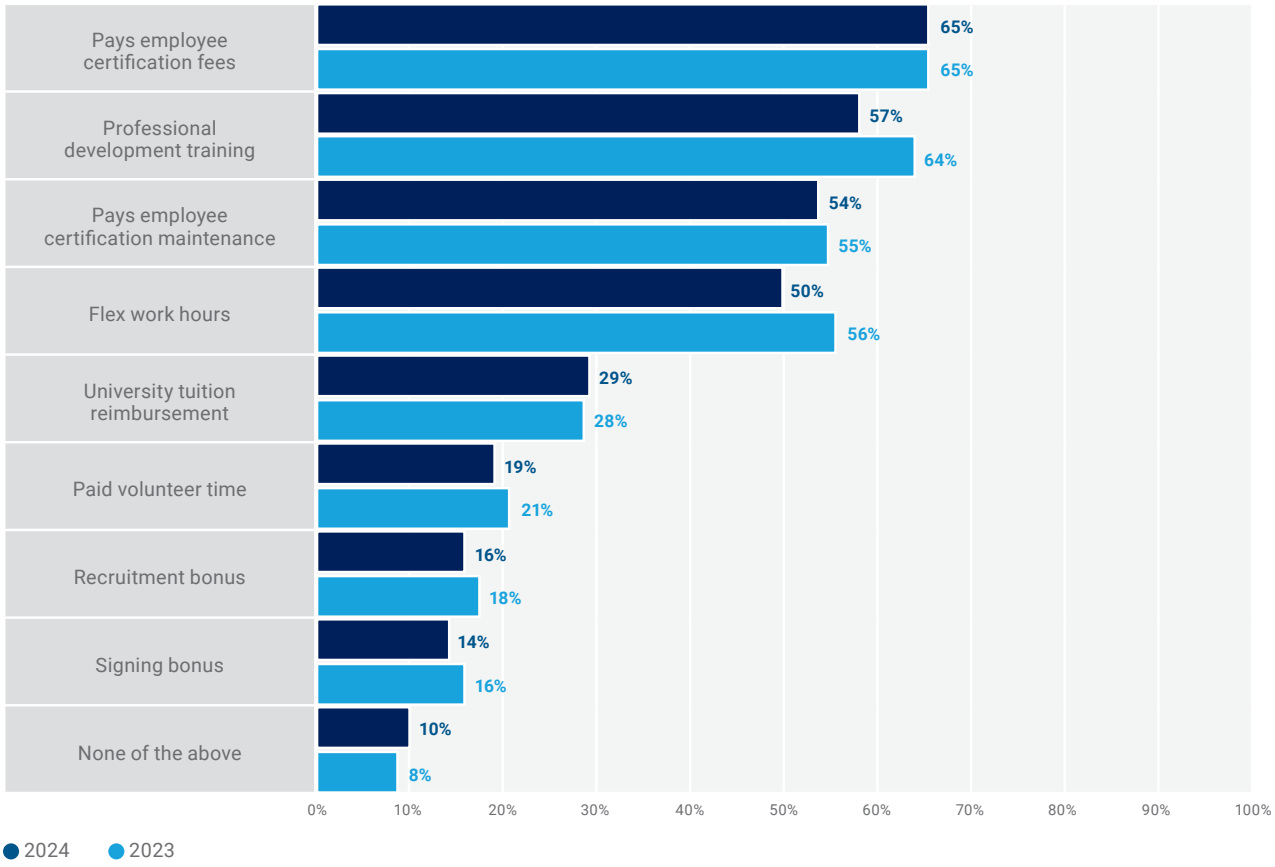


FIGURE 16: Employer Benefits

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



Pipeline Progress

Qualifying Applicants

Respondent views on whether candidates are well qualified for vacancies[9] crept up slightly by two percentage points from last year to 28 percent (**figure 17**).

Figure 18 shows that prior hands-on cybersecurity experience dominates as the primary factor (73 percent) in determining whether a candidate is considered qualified. Views on credentials and hands-on training are unchanged. Respondents place less emphasis on prior-employer recommendations and university degrees than last year—each fall three percentage points. Surprisingly, the importance of association membership climbed four percentage points.

Respondents report that although soft skills continue to dominate all other skill gaps (51 percent), soft skills decrease four percentage points from last year's survey results. Respondents report betterments in cloud

9 Derived from a combination of the 50-75% and 76-100% responses.

FIGURE 17: 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?

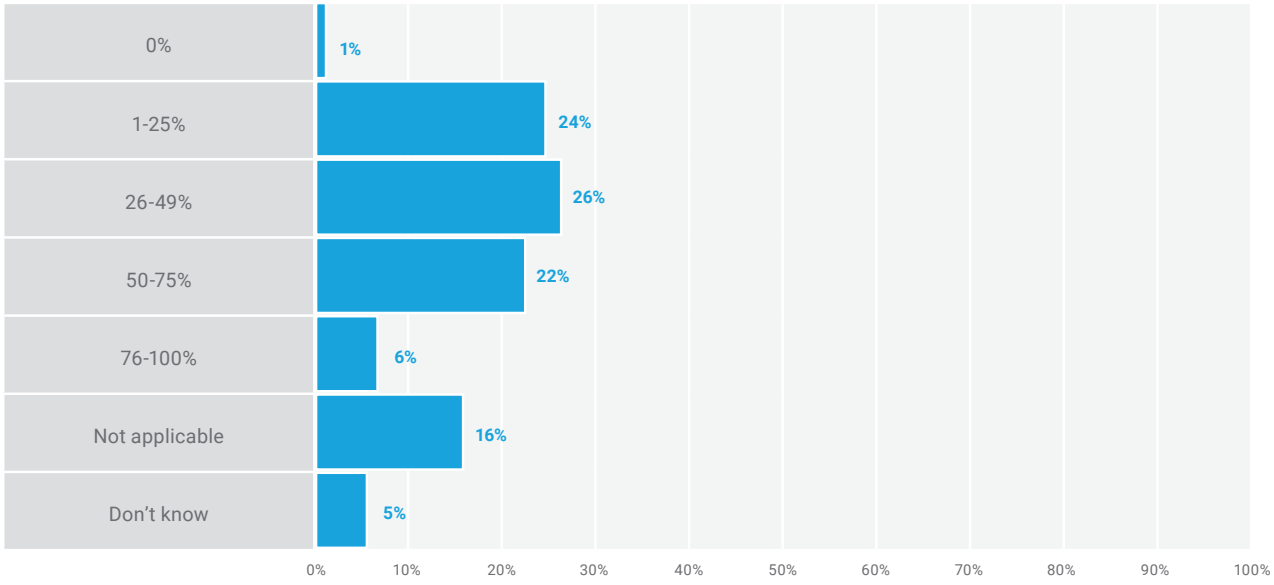
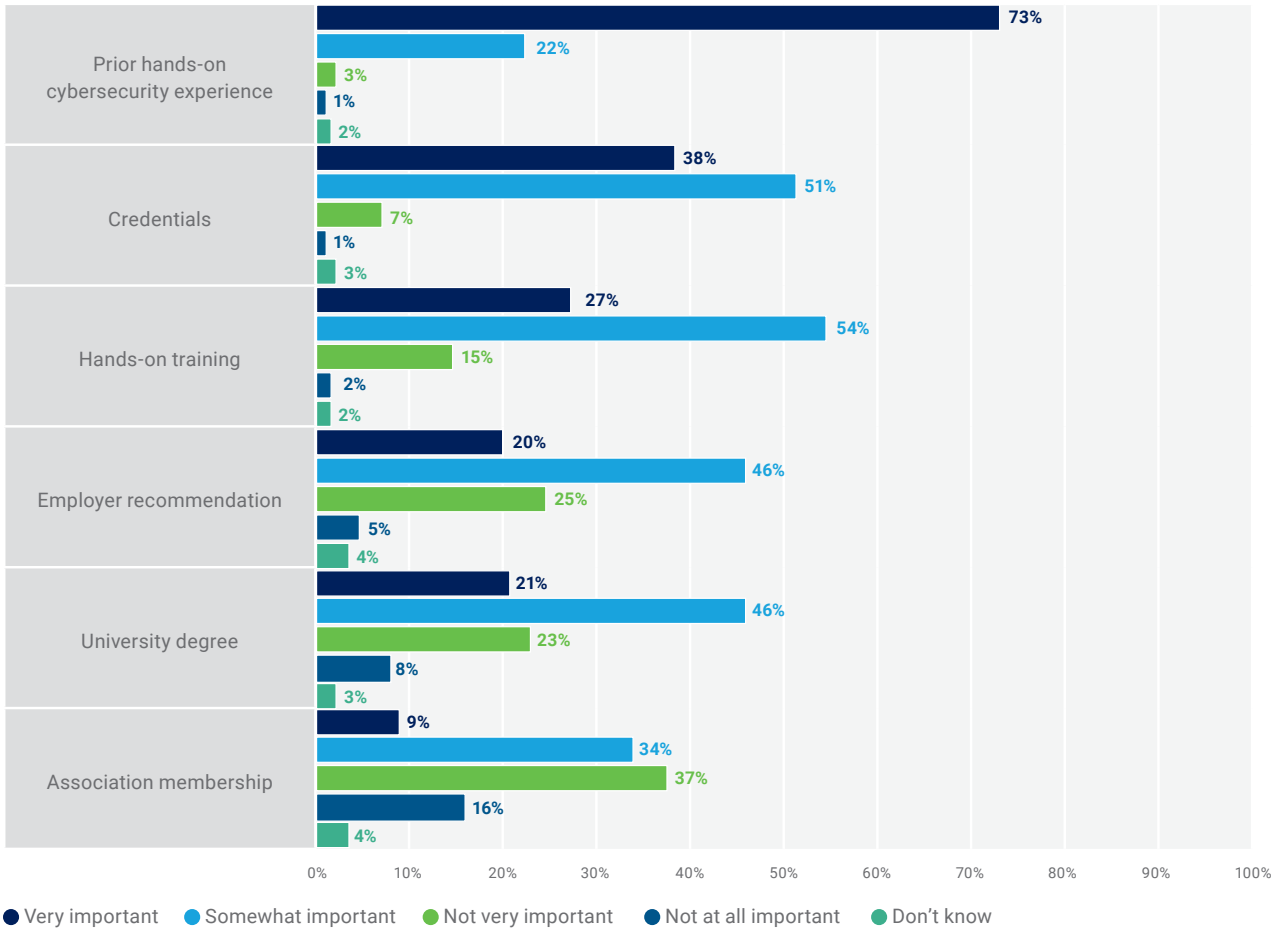


FIGURE 18: Candidate Qualifications

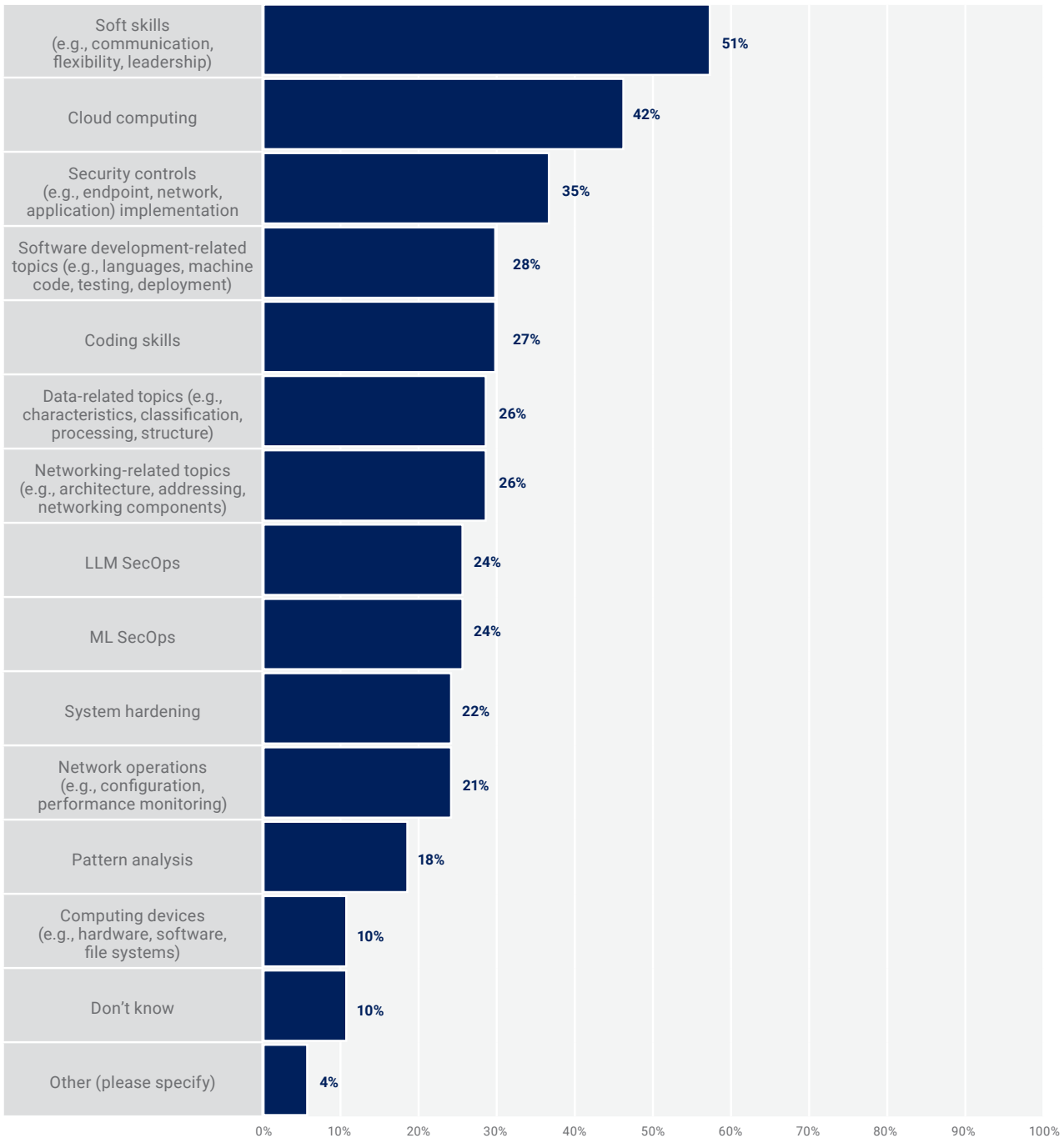
How important are each of the following factors in determining if a cybersecurity candidate is qualified?



computing (down five percentage points); coding (down three percentage points); and software development-related topics, data-related topics, and pattern analysis—each down two percentage points. Security controls (35 percent), network operations (21 percent), and computing devices (10 percent) are unchanged. New for 2024, two response options—LLM SecOps and ML SecOps—are added to this question. Twenty-four percent of respondents select these skill gaps (**figure 19**).

FIGURE 19: Quantified Skill Gaps

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



University Insights

Respondent views about whether recent university graduates are well prepared for enterprise cybersecurity challenges are unchanged from last year (**figure 20**), yet the percentage of respondent enterprises requiring a degree to fill entry-level cybersecurity positions (**figure 21**) increases three percentage points (55 percent). When asked about skill gaps among recent university graduates, respondent views are mixed, but soft skills and security controls remain the top-two skill gaps observed by respondents (**figure 22**). To keep current with advancements in security operations, ML SecOps and LLM SecOps are added to the response options for the skill gaps question in the 2024 survey. Seventeen percent of respondents believe that these are skill gaps.

Regional requirements for a university degree vary. Africa saw a seven percentage-point climb (76 percent) in the requirement, which may be due to the small sample size. European respondents continue to be reluctant to require a university degree for entry-level cybersecurity positions and report another incremental decrease (43 percent). Europe is second only to Oceania (38 percent).

FIGURE 20: 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?

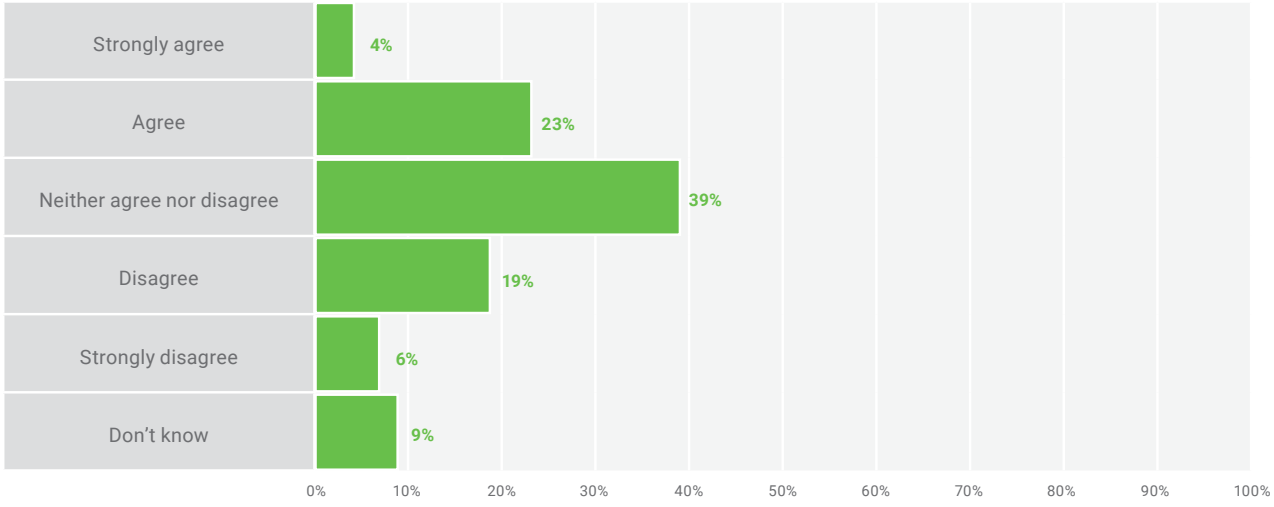


FIGURE 21: University Requirement

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

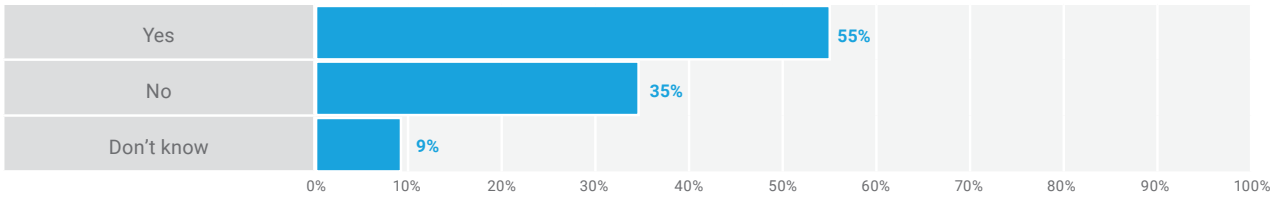
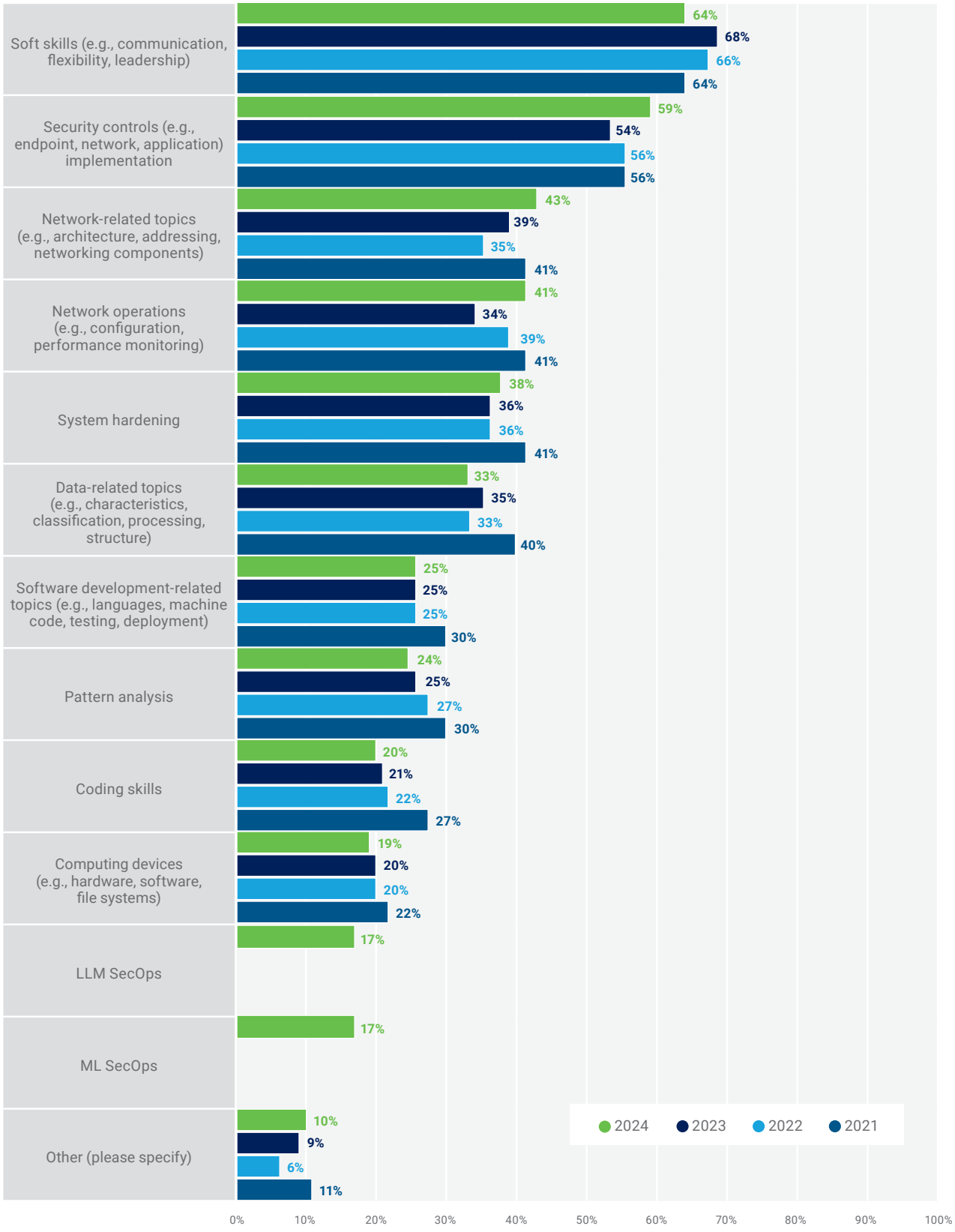


FIGURE 22: Skill Gaps Among Recent Graduates[10]

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



10 LLM SecOps and ML SecOps are new response options in 2024.

Qualifying Workforce Issues

For 2024, the reported top-three security skills change (**figure 23**). Data protection (46 percent) overtakes identity and access management (45 percent), while incident response (44 percent) ranks higher than cloud computing (43 percent) in this year's survey results. DevSecOps falls eight percentage points (28 percent); data collection/correlation (30 percent) and threat hunting (26 percent) drop three percentage points; and forensics drops two percentage points (18 percent). Ten percent of respondents believe that the newly added responses, ML SecOps and LLM SecOps, belong in the top-five most important security skills needed in their enterprises.

Respondent reporting about required soft skills for security professionals (**figure 24**) shows that communication (both listening and speaking skills) (56 percent), critical thinking (54 percent), and problem solving (50 percent) remain the top-three required soft skills. The survey results show a concerning trend in ethics—attention to detail (35 percent) falls three percentage points since 2022, honesty (15 percent) continues not to be recognized as sufficiently important, and empathy (11 percent) drops two percentage points.

Survey results show a concerning trend in ethics—attention to detail falls three percentage points since 2022, honesty continues not to be recognized as sufficiently important, and empathy drops two percentage points.

Professional Development Needs by Career Stage

Respondent data shows that the top-three areas where staff with less than three years of work experience (early career) require the most professional development/training are security controls (58 percent), soft skills (55 percent), and cloud computing (44 percent). Security controls and soft skills improved by three and five percentage points, respectively, from 2023 survey results.

When comparing this early-career group against university graduates and those with more experience (**figure 25**), a prevailing theme surfaces for many training areas—proficiency improves markedly as individuals advance in their careers, which is logical. This theme diverges with cloud computing, software development-related topics, coding, ML SecOps, and LLM SecOps because early-career professionals have greater perceived proficiency than the career groups above and below them. In an era where professional development budgets are often targets for cost savings, this observation underscores the need for continuous learning/upskilling—especially on emerging technology—for employees who have been in the cybersecurity profession for a longer time.

Human Capital Mitigations

Forty-one percent of respondents indicate that their enterprises leverage training to allow interested nonsecurity professionals to move into security roles as a method of mitigating skill gaps. Respondents report decreased usage of contracted help or outside consultants (36 percent) to help decrease skill gaps. After a sizeable decline in 2023, reliance on AI or automation rebounds to 23 percent. Reskilling programs (21 percent), use of performance-based training, and credentials (19 percent) remain unchanged, while the use of apprenticeship programs (16 percent) slid three percentage points (**figure 26**).

FIGURE 23: Top Five Security Skills

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

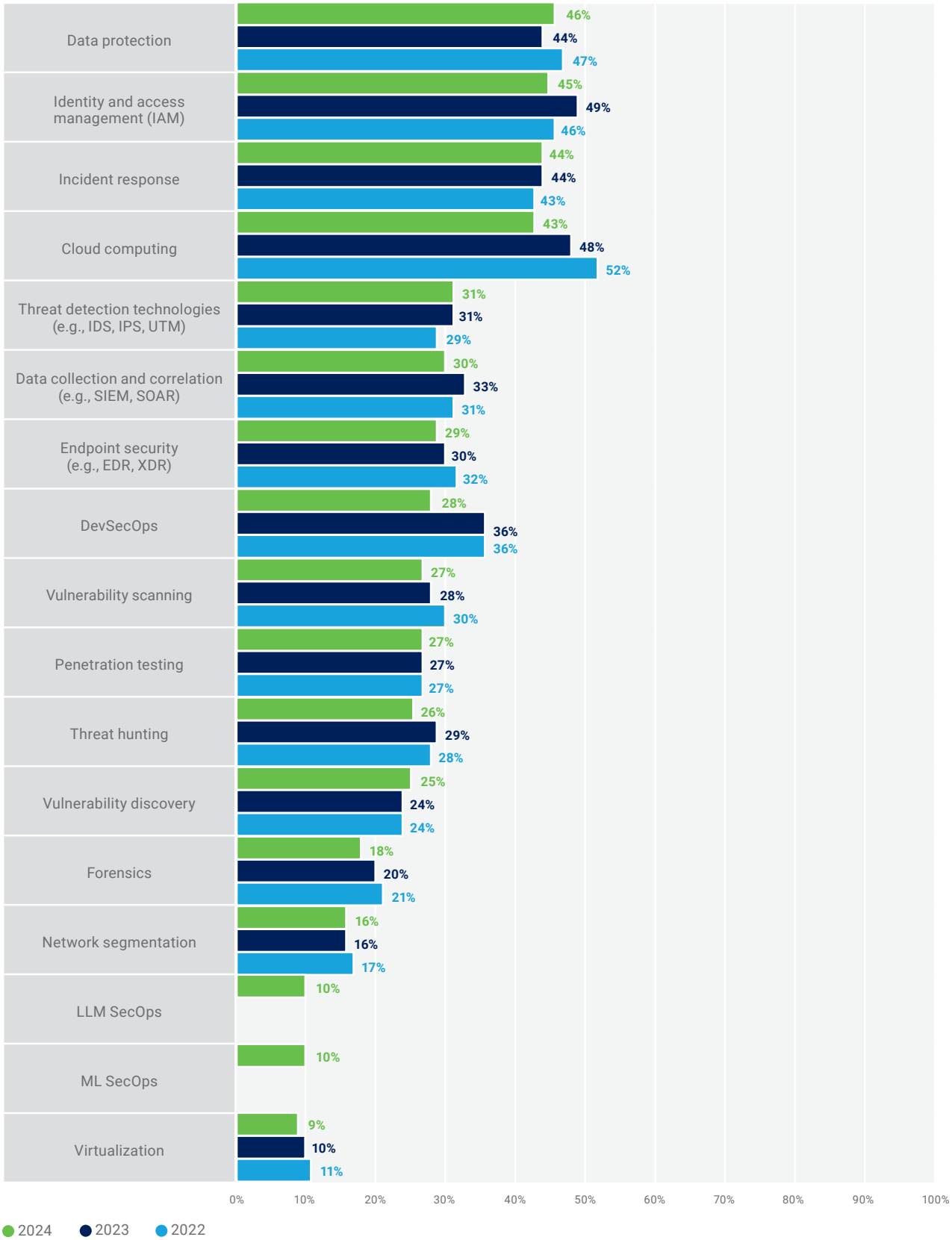


FIGURE 24: Top Five Soft Skills

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

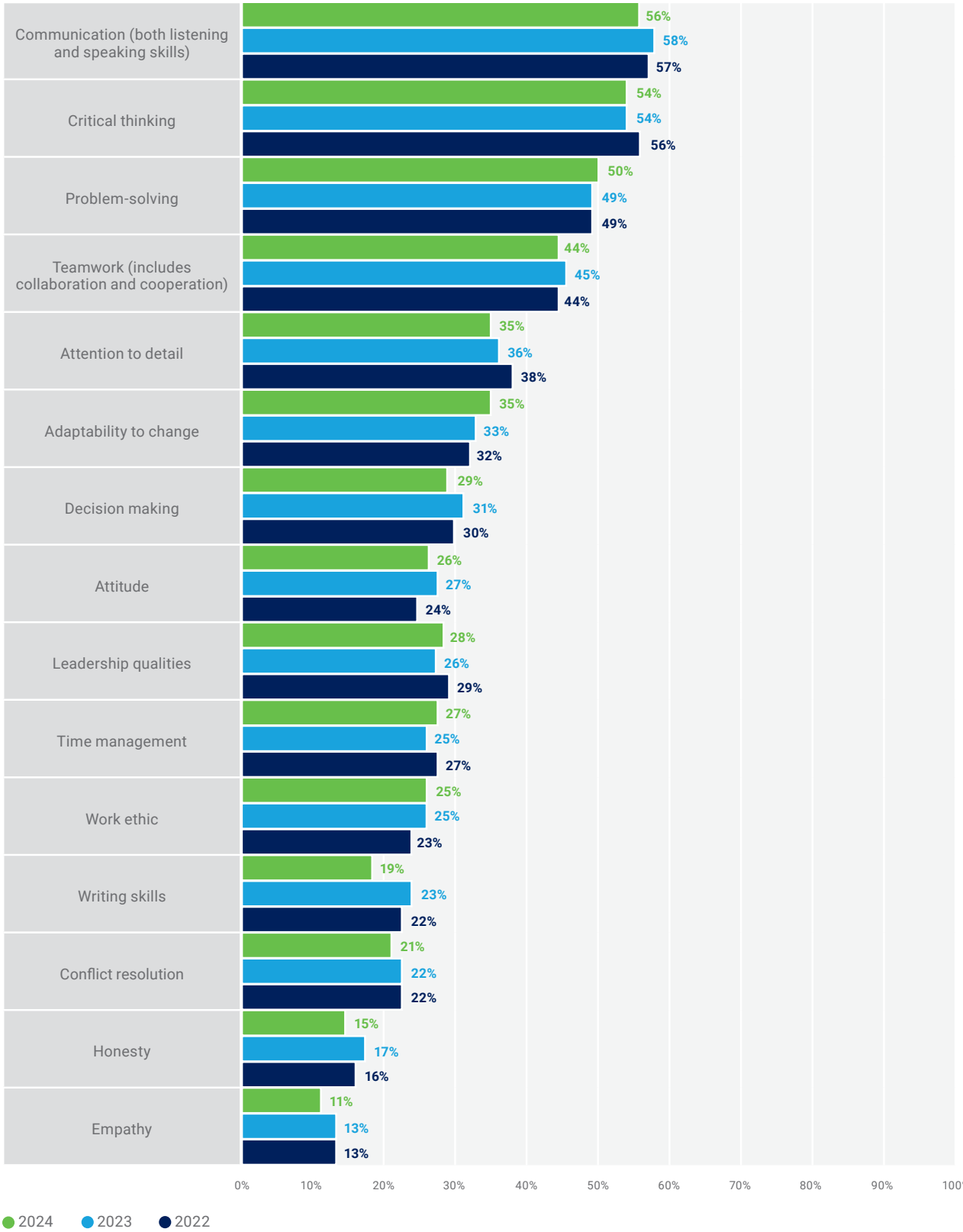
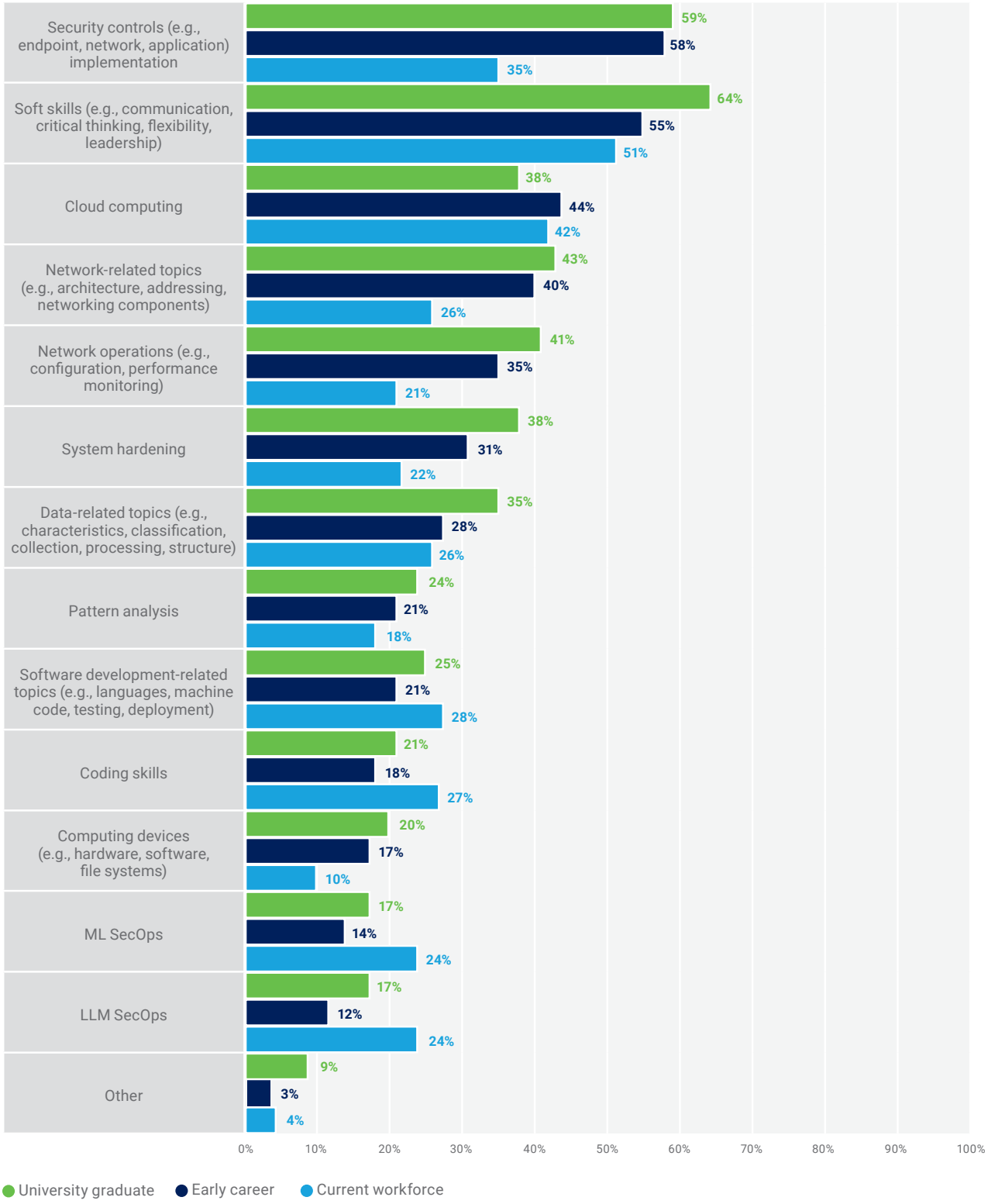


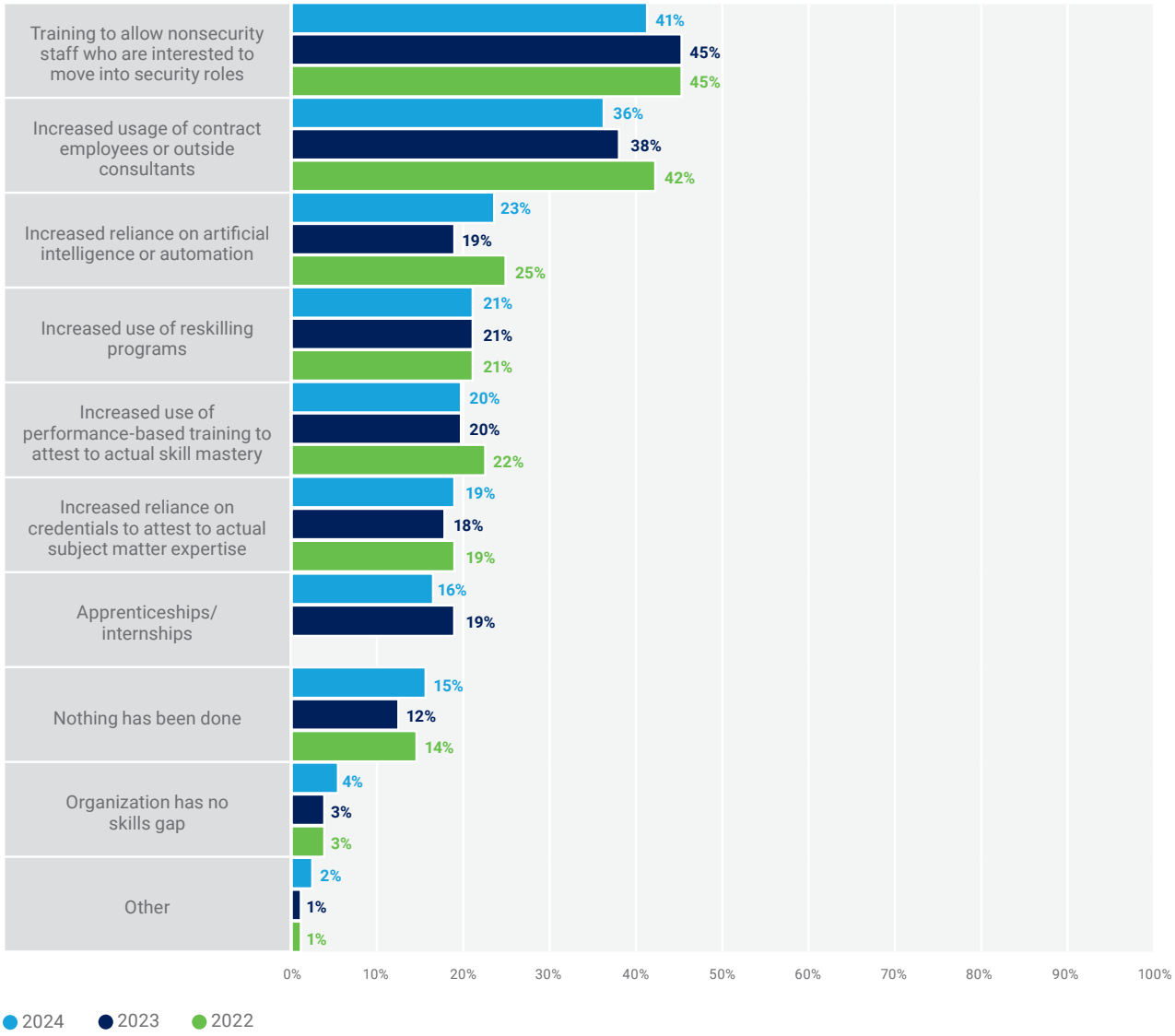
FIGURE 25: Professional Development Needs by Career Stage[11]



11 This chart is a comparative analysis based on respondent views about which professional development/training areas are MOST needed by university graduates, early career, and all others.

FIGURE 26: Means of Mitigating Technical Skill Gaps

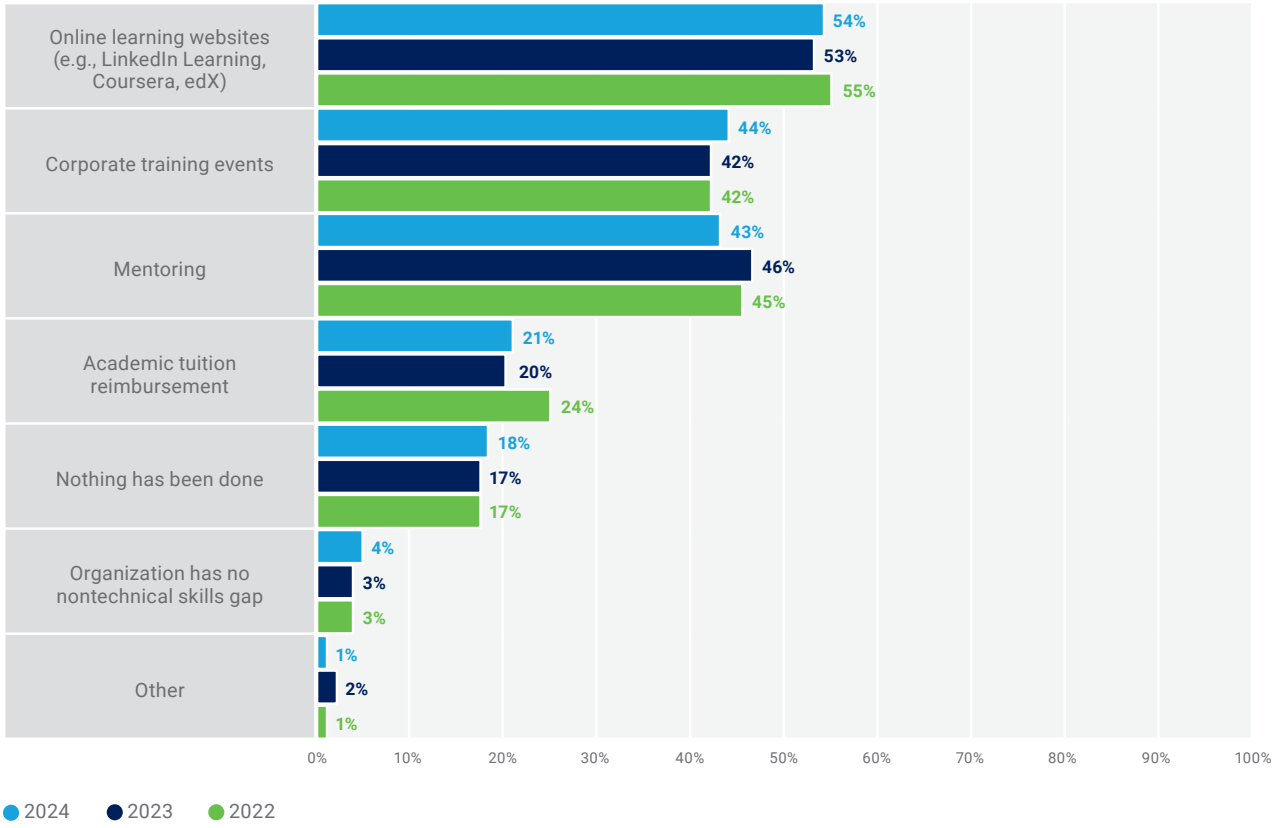
Which, if any, of the following has your organization undertaken to help decrease technical cybersecurity skills gaps? Select all that apply.



Organizations continue to leverage online learning websites primarily (54 percent) to increase nontechnical skills of staff. Corporate training events increases two percentage points (44 percent), while mentoring (43 percent) declines three percentage points from 2023 survey results. **Figure 27** shows employer actions to overcome soft skills shortcomings.

FIGURE 27: Means of Mitigating Nontechnical Skill Gaps

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



Cybersecurity Budgets in Decline

After two years of respondents strongly feeling that budgets are appropriately funded, data show a significant drop in cybersecurity funding levels (**figure 28**). Thirty-six percent of respondents indicate that their budgets are appropriately funded, which is a five percentage-point drop from last year; forty-four percent of respondents feel that their budgets are somewhat underfunded, which is an increase of four percentage points. When asked how they expect budgets to change in the next 12 months, respondent data are bleak (**figure 29**). Only 47 percent of respondents believe that budgets will increase (down four percentage points), while 41 percent (an increase of three percentage points) of respondents say that budgets will remain the same. Thirteen percent of respondents expect budgets to shrink over the next year—a view that is incrementally growing since 2022. The nine-year outlook on enterprise security budgets no longer shows leveling, instead shows a potential multiyear freefall (**figure 30**).

FIGURE 28: Cybersecurity Funding Perception

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

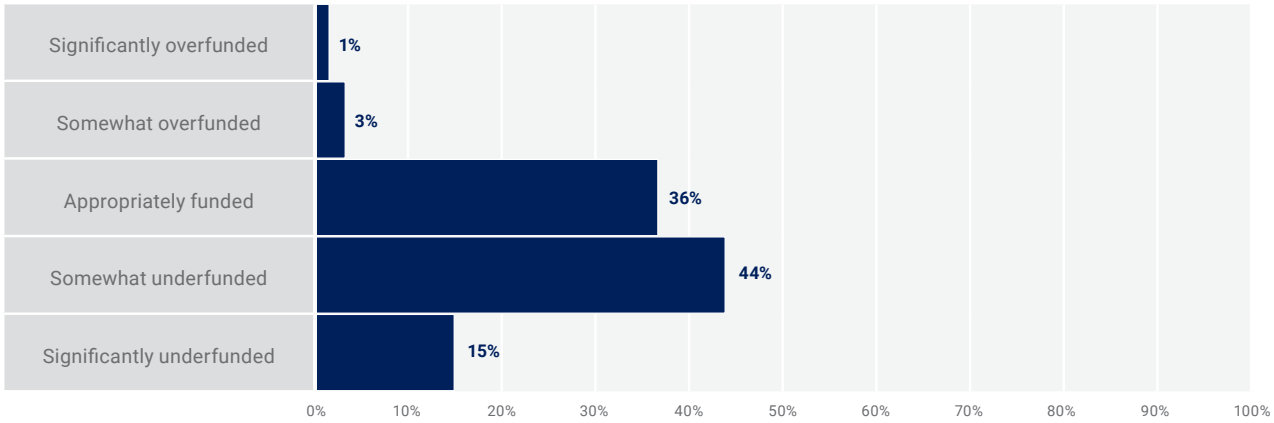


FIGURE 29: Enterprise Security Budget Outlook

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

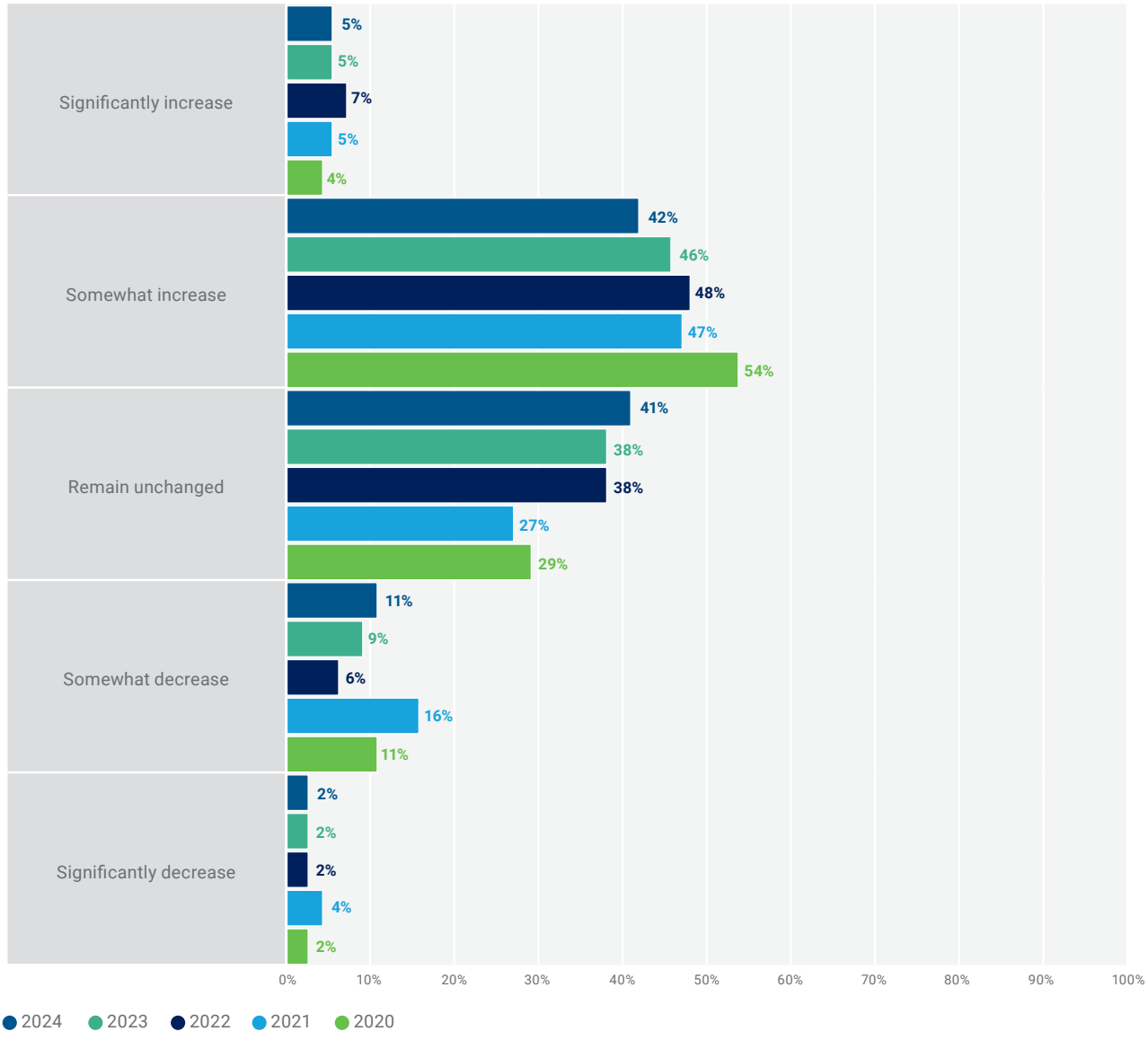
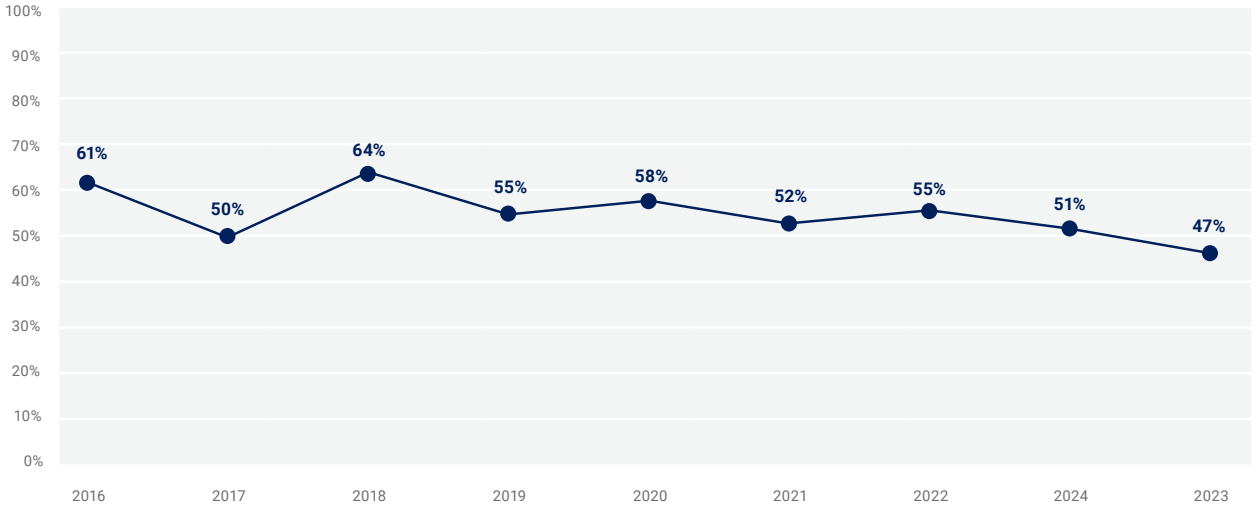


FIGURE 30: Forecasted Security Budget Increases (9 Year)

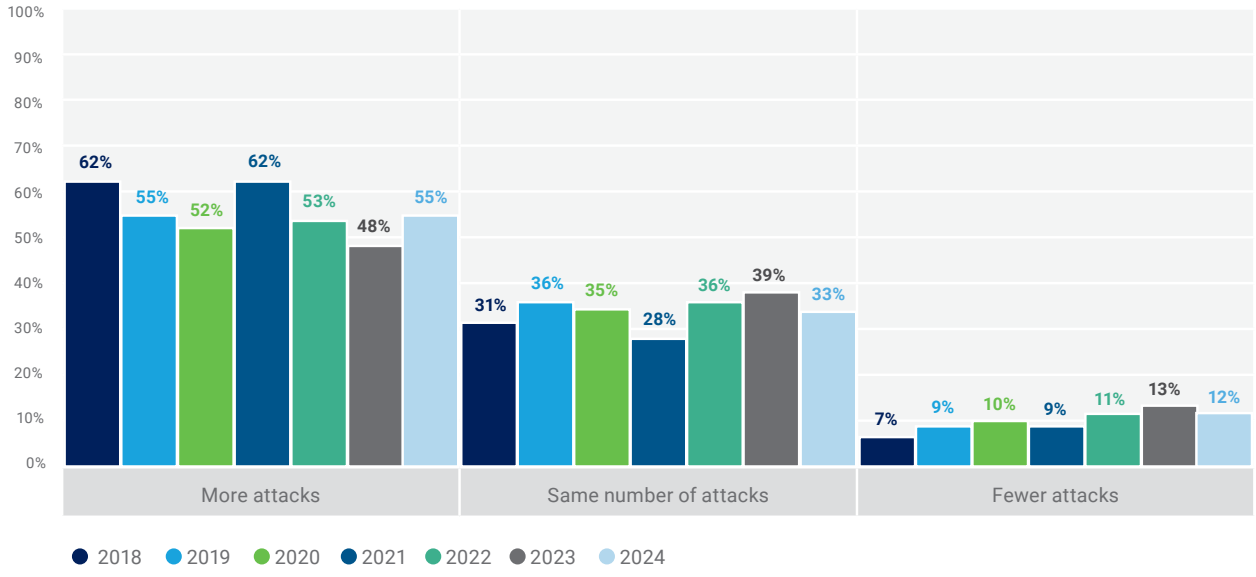


Cyberattacks, Detection, and Threat Actors

Respondent organizations are experiencing more cyberattacks compared to a year ago. **Figure 31** shows a seven-year trend.

Confidence levels surrounding the ability of respondent organizations to respond to cyberthreats show no notable change from 2023 (**figure 32**).

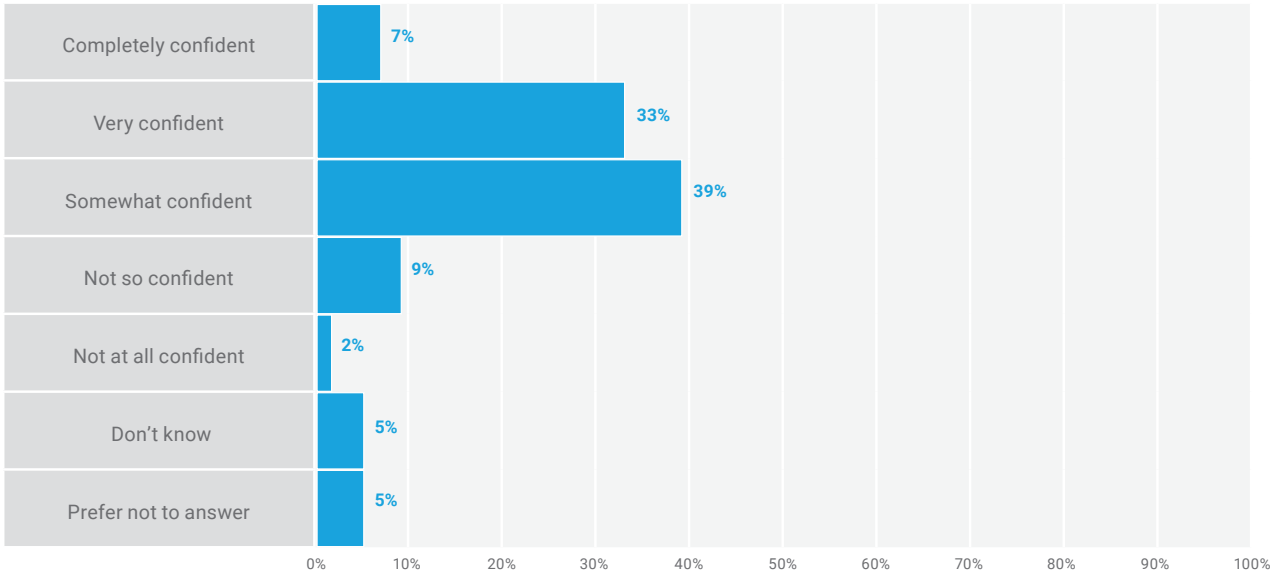
FIGURE 31: Year Over Year Comparison of Cybersecurity Attack Reporting[12]



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

FIGURE 32: Organizational Confidence

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



Nearly half of respondents believe that their enterprises will experience a cyberattack next year (**figure 33**), which is similar to last year's survey results.

Data surrounding threat actors nearly mirror last year's data and are consistent with prior-year survey results (**figure 34**), with two minor differences. Nonmalicious insider exploits drop two percentage points (nine percent), which is an acceptable metric that is likely attributed to cybersecurity training and awareness programs and insider-threat awareness education.

The respondents selecting the "Not applicable" answer declines three percentage points to 23 percent, which is not surprising given an increasingly complex threat landscape.

Nearly half of respondents believe that their enterprises will experience a cyberattack next year.

The use of social engineering as an attack vector increases four percentage points (19 percent) and remains the prominent type of attack. **Figure 35** shows the attack types that hackers used to successfully exploit respondent enterprises.

FIGURE 33: Likelihood of Attack

How likely is it that your organization will experience a cyberattack next year?

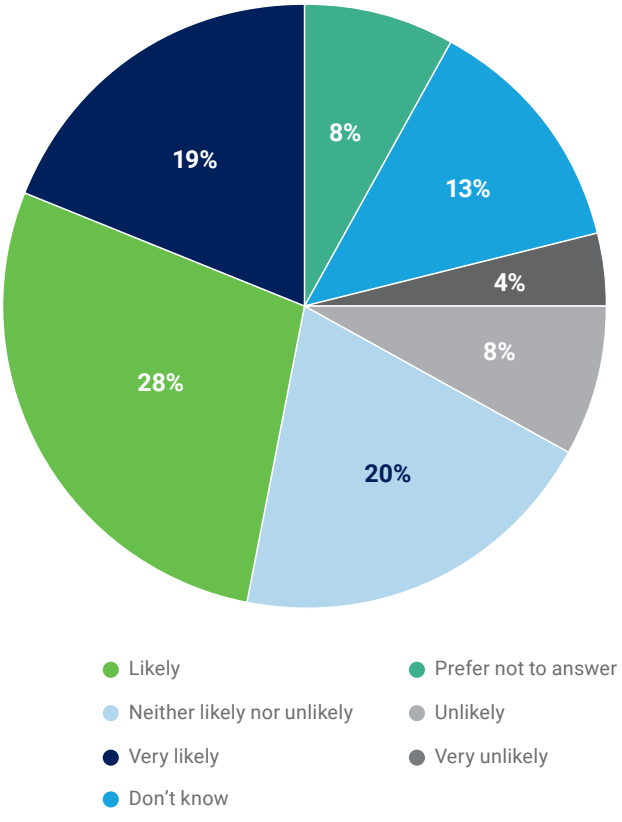
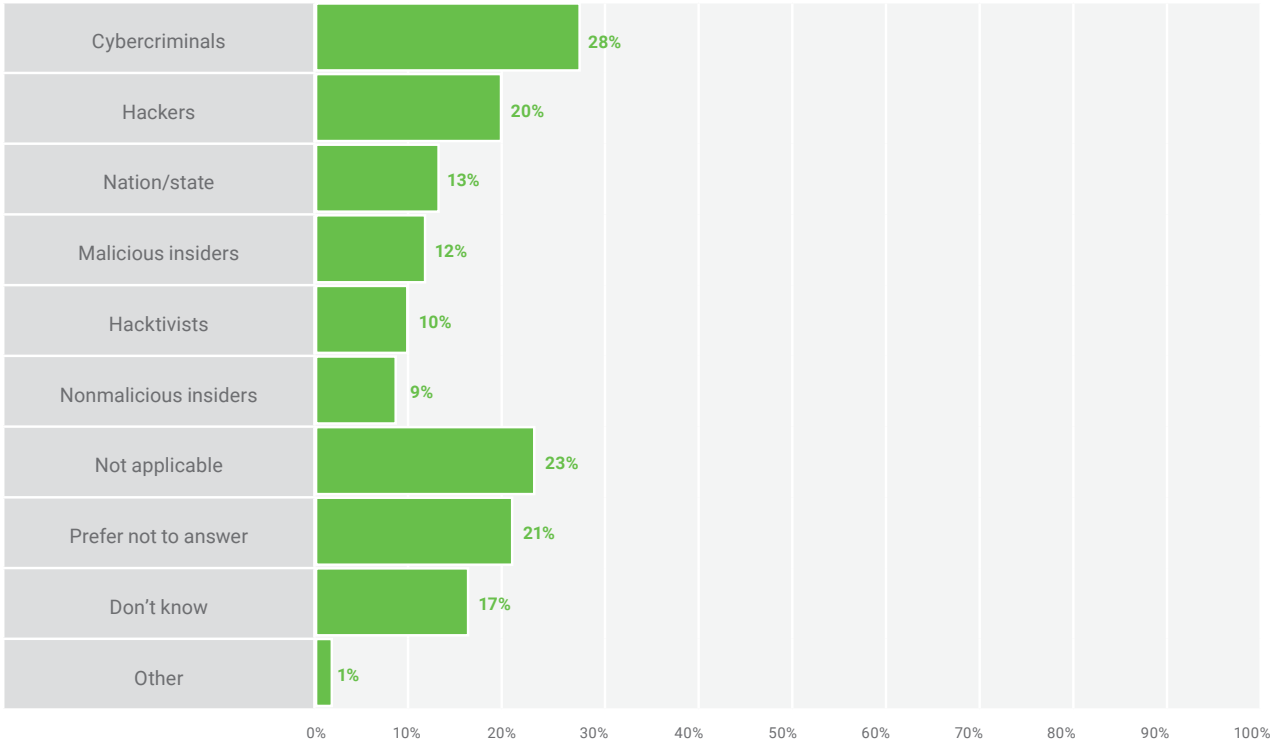


FIGURE 34: Threat Actors

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



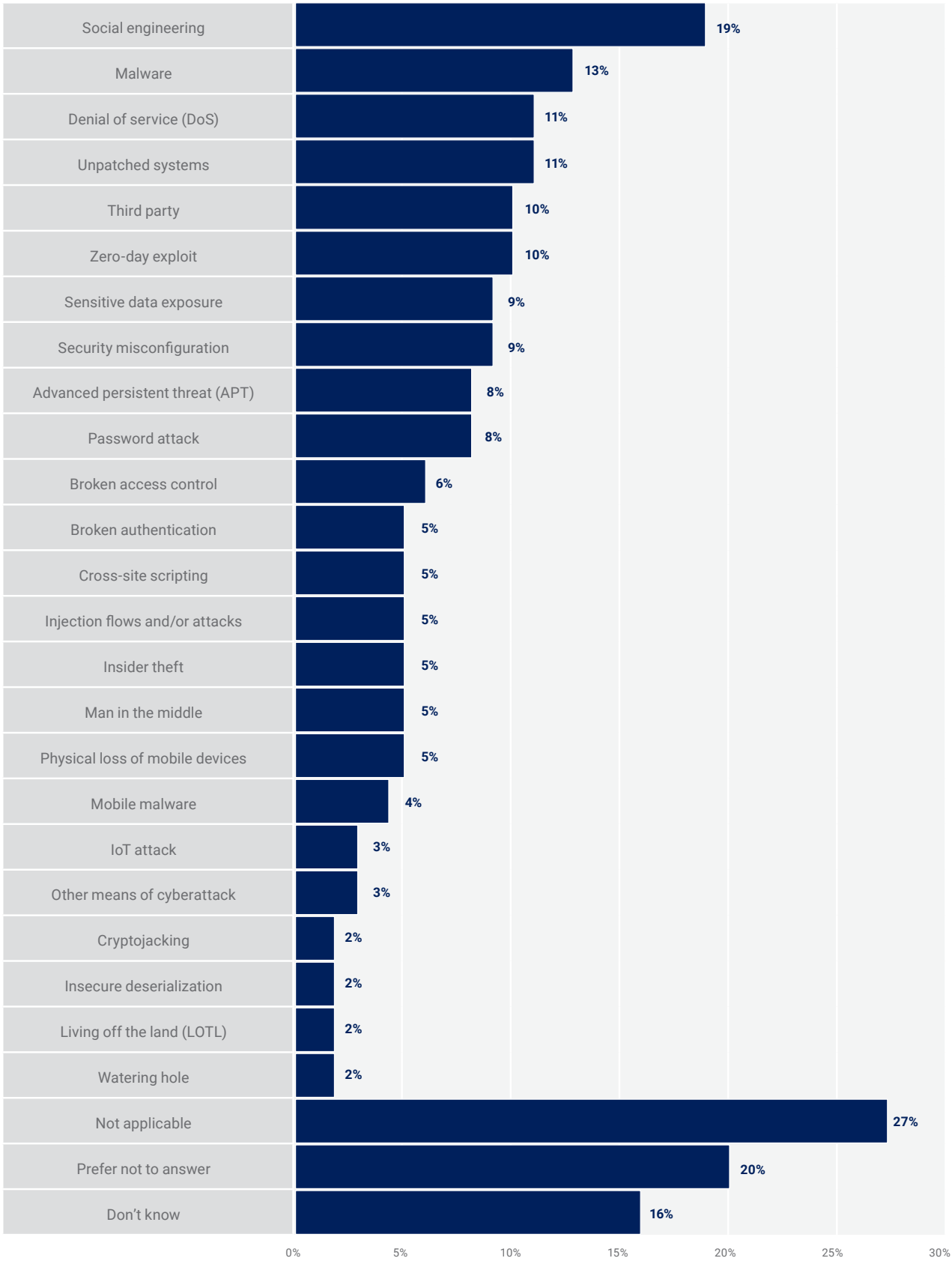
Data surrounding threat actors nearly mirror last year's data and are consistent with prior-year survey results.

Nonmalicious insider exploits drop two percentage points—an acceptable metric that is likely attributable to cybersecurity training and awareness programs and insider-threat awareness education.

The use of social engineering as an attack vector increases four percentage points and remains the prominent type of attack.

FIGURE 35: Attack Types

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



Cyberrisk

Respondent beliefs about whether their board of directors adequately prioritizes cybersecurity remains unchanged this year. Fifty-six percent of respondents believe that their board of directors adequately prioritizes enterprise cybersecurity. Nine percent of respondent executive-leadership teams do not find value in conducting cyberrisk assessments (**figure 36**), which is surprising in the current era of cyberattacks.

Forty-one percent of respondent enterprises conduct cyberrisk assessments annually (**figure 37**), which is a two-point increase from last year. All other response options, except "Don't know," remain unchanged. Respondents indicating "Don't know" decreases three percentage points from last year's survey results.

Enterprises face many obstacles to performing cyberrisk assessments. The percentage of respondent enterprises affected by these barriers are largely unchanged from last year. Time commitment remains key (41 percent); however, lack of internal expertise increases two percentage points (24 percent) and lack of funds to outsource to a third party increases four percentage points (18 percent) from 2023.

FIGURE 36: Executive Leadership Value

Does your executive leadership team see value in conducting a cyberrisk assessment?

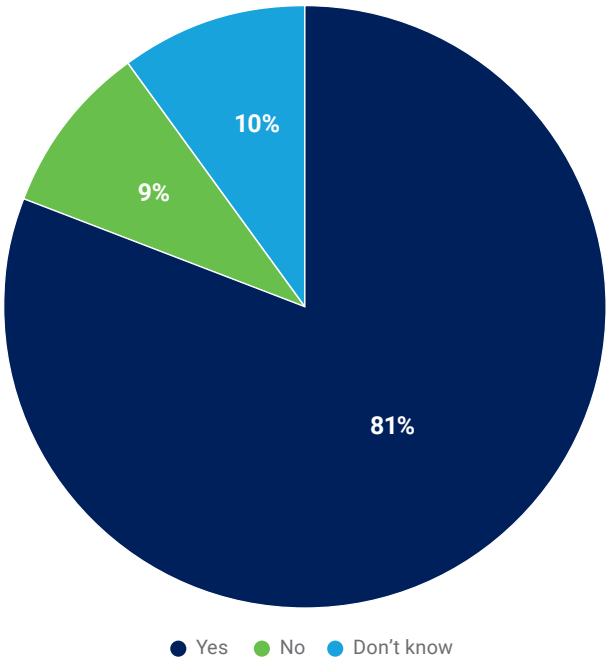
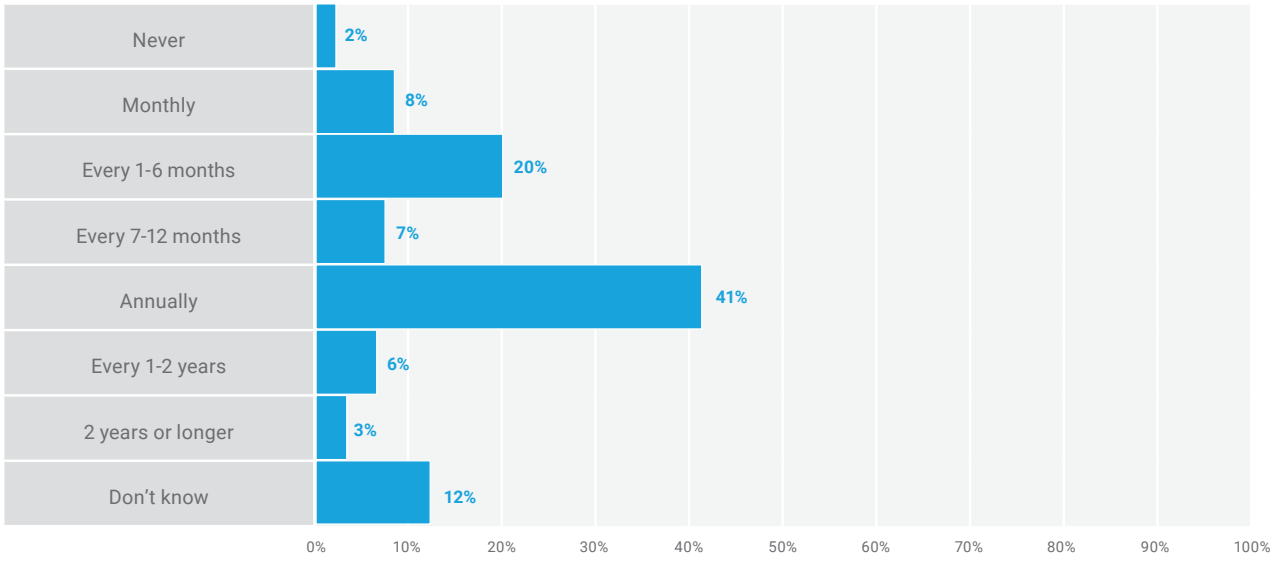


FIGURE 37: Cyberrisk Frequency

How often is a cyberrisk assessment performed on your organization?



Cyberinsurance

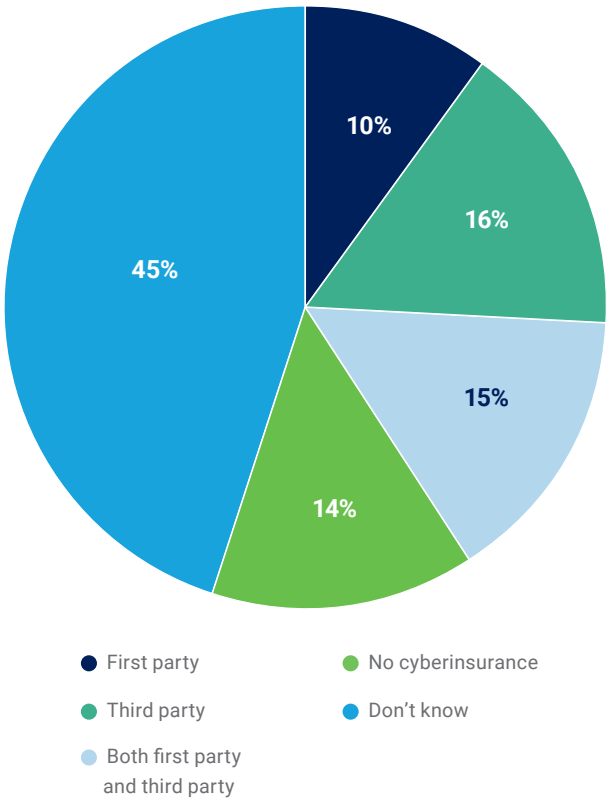
The topic of cyberinsurance is added to the *State of Cybersecurity Survey* in 2024. The cyberinsurance questions ask respondents about their knowledge of the type of cyberinsurance that their enterprise purchased, whether the policy is adequate to address cyberrisk, and whether their enterprise cyberinsurance policy was ever used.

Ten percent of respondents report that their enterprise has first-party cyberinsurance (**figure 38**), which generally covers the costs associated with investigating and responding to cyberevents and includes the financial impact on business operations. Sixteen percent of respondents report that their enterprise has only third-party cyberliability insurance, which addresses financial indemnity to the enterprise for claims of damages resulting from a cyberevent.[13] Fifteen percent of respondents indicate that their enterprise has first-party and third-party cyberinsurance. Fourteen percent of respondent enterprises do not carry cyberinsurance.

The bigger story in the data is that almost half of the survey respondents do not know what kind of cyberinsurance their enterprise carries. Survey results show a relationship between respondent knowledge of enterprise cyberinsurance and enterprise size; specifically, the greatest number of respondents report no knowledge about their enterprise cyberinsurance work for enterprises with more than 10,000 employees. From a regional perspective, 57 percent of those in Oceania lacked knowledge of enterprise cyberinsurance type, followed by North America (49 percent) and Europe (43 percent). Although views may vary about whether cybersecurity professionals need to know the type of cyberinsurance carried by the enterprise, the benefits to having this knowledge include the ability to help plan for incidents and other claimable events, and their subsequent responses (e.g., incident response playbooks). Considering that an enterprise risk profile highly influences cyberinsurance premiums,[14] not knowing can result in organizational dismay if expectations surrounding coverage go unmet. Lastly, insurers increasingly require minimal levels of care; therefore, close collaboration between those who secure cyberinsurance for the enterprise and key security professionals can help decrease the risk profile and improve rates.

FIGURE 38: Cyberinsurance Type

What kind of cyberinsurance, if any, does your organization carry?



13 Vaideeswaran, N.; "Cyber Insurance Explained," 22 February 2024, www.crowdstrike.com/cybersecurity-101/cyber-insurance/

14 Bedard, T.; "Cyber Insurance: Why You Need It and What to Look for in a Policy," proofpoint, 20 May 2024, www.proofpoint.com/us/blog/email-and-cloud-threats/what-to-look-for-cyber-insurance-coverage

Ninety-six percent of respondents in enterprises that have cyberinsurance report that their enterprise cyberinsurance policy at least somewhat addresses their enterprise risk profile (**figure 39**). One-third of these respondents report that their enterprise used its cyberinsurance policy (**figure 40**). Of those respondents who are aware that their enterprise used its cyberinsurance policy, most believe that their policy has complete coverage.

FIGURE 39: Adequacy of Cyberinsurance

Does your organization's cyberinsurance policy adequately address your risk profile?

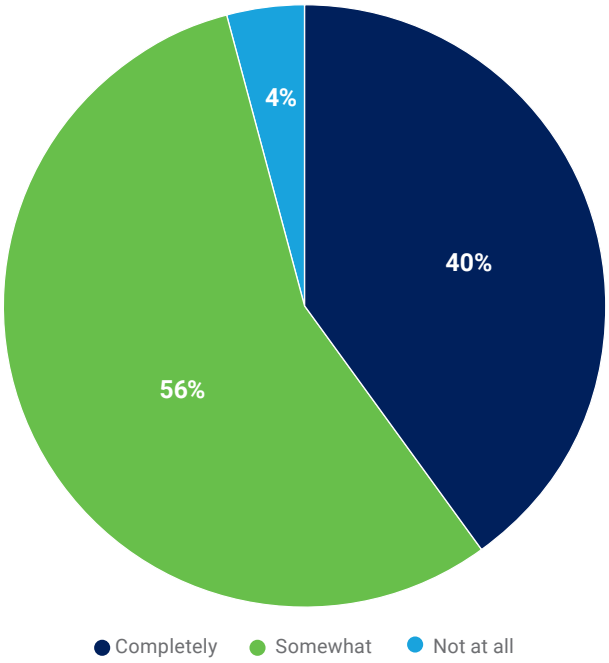
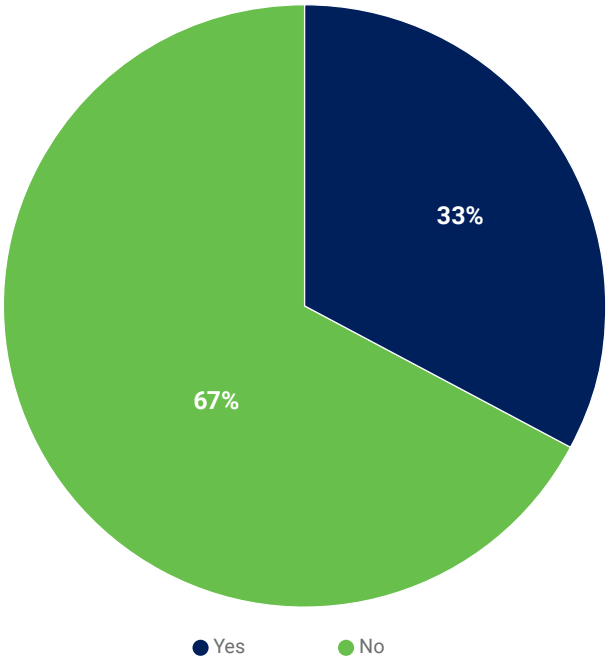


FIGURE 40: Utilization of Cyberinsurance

Has your organization ever used its cyberinsurance policy?



Insurers increasingly require minimal levels of care; therefore, close collaboration between those who secure cyberinsurance for the enterprise and key security professionals can help decrease the risk profile and improve rates.

Security Operations: Focus on Artificial Intelligence

Roughly one-third of respondent enterprises have security teams consisting of more than 25 individuals (**figure 41**); however, the average size of staff is 16 individuals.

ISACA added questions about the use of AI in security operations to the *State of Cybersecurity Survey* in 2024. **Figure 42** shows how AI is being used in respondent enterprise security operations. Automating threat detection/response (28 percent) and endpoint security (27 percent) are the most popular applications of AI. Those respondents reporting that their enterprise is increasing reliance on AI or automation to decrease the cybersecurity technical skills gap still say that their cybersecurity teams do not have enough workers.

FIGURE 41: Security Team Size

Please indicate the size of your security staff.

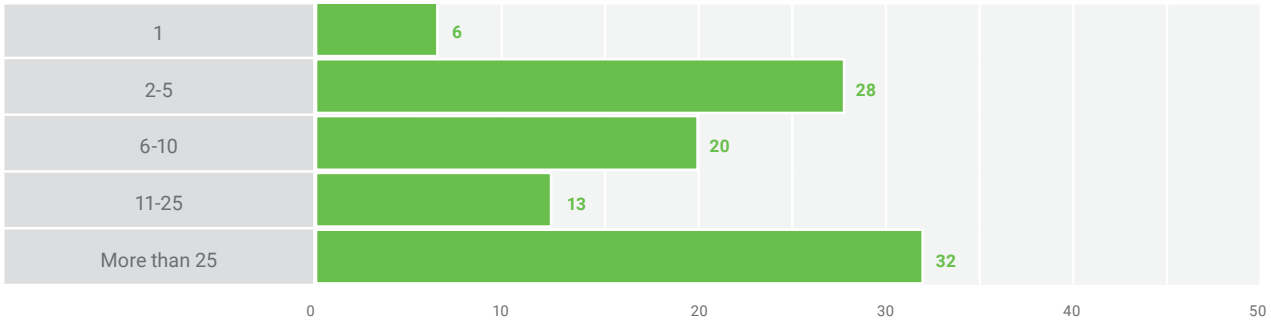
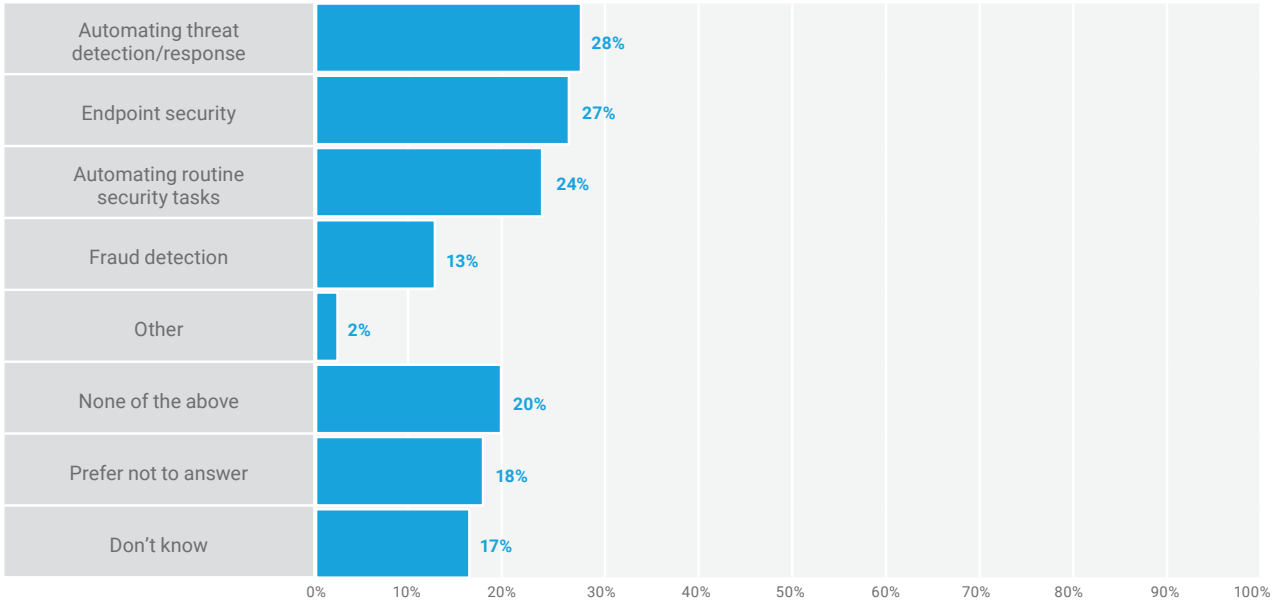


FIGURE 42: AI Use in Security Operations

Does your organization use AI in any of the following security operations?



Security operations is just one of the areas in which AI can help enterprises. ISACA sought to understand how respondents are involved with AI policies and onboarding solutions for other areas of the business.

When asked whether the respondent or anyone on their team was involved in the development, onboarding, or implementation of AI solutions, the respondent answers are disheartening (**figure 43**). Nearly half (45 percent) of respondents report no involvement, which holds true for Europe, India, Latin America, North America, and Oceania data. Twelve percent of respondents indicate that the question does not apply to their organization. Responses are similar across cybersecurity staffing and budgetary views. Respondents in enterprises with more than 10,000 employees report less involvement than respondents in smaller organizations, which is understandable and provides an opportunity to increase collaboration and transparency in decision making.

When asked whether the respondent or anyone on their team was involved in the development of a policy governing the use of AI technology in their enterprise (**figure 44**), the respondent answers are equally disappointing. Only 35 percent of respondents report involvement. Ten percent of respondents indicate that the question does not apply. Respondents who are employed by enterprises with 500-to-4,999 employees report greater involvement than respondents employed by enterprises with fewer than 500 employees.

FIGURE 43: Involvement of AI Life Cycle

Were you, or anyone on your team, involved in the development, onboarding, or implementation of AI solutions?

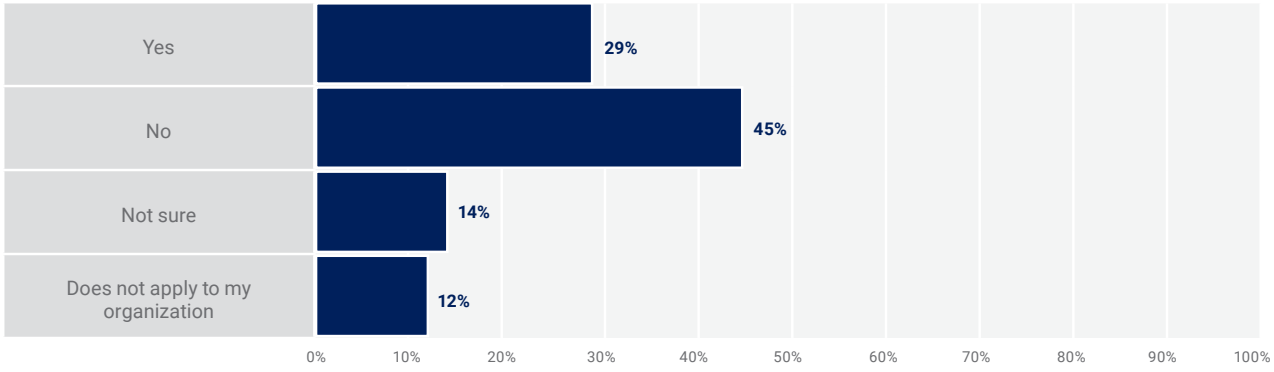
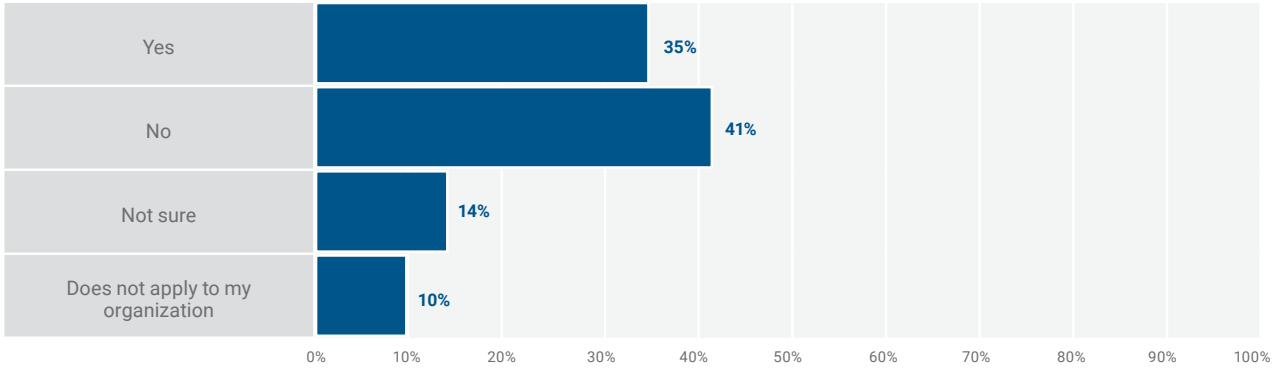


FIGURE 44: Involvement in AI Policy

Were you, or anyone on your team, involved in the development of a policy governing the use of AI technology in your organization?



Conclusion: Focus on Cybersecurity Readiness

The ISACA global *State of Cybersecurity Survey* has been conducted for a decade. Although 10 years is a relatively long time for a comparatively new profession, some of the challenges reported from the survey have not changed much over these 10 years.

The demand for cybersecurity talent has been consistently high, yet efforts to increase supply are not reflected in the global ISACA IS/IT-community workforce. The current cybersecurity practitioners are aging, and the efforts to increase staffing with younger professionals are making little progress. Left unchecked, this situation will create business continuity issues in the future.

Shrinking budgets and employee compensation carry the potential to adversely affect cybersecurity readiness much sooner than the aging workforce, when the Big Stay passes. Declines in vacant positions across all reporting categories may lead some enterprises to believe that the pendulum of power will swing back to employers, but the increasingly complex threat environment is greatly increasing stress in cybersecurity teams; therefore, the concern is not if, but when, employees will reach their tipping point to vacate current positions.

Although nearly half of respondents indicate that their enterprises leverage training to allow interested nonsecurity professionals to move into security roles, declining professional development training budgets are concerning. This approach may also demotivate existing staff. The significant drop in cybersecurity funding levels reported this year points to the beginning of a multiyear freefall.

Although this year's survey data show fewer exploitations attributed to nonmalicious insiders, effective insider-threat and cybersecurity training and awareness programs alone do not protect enterprises in today's everchanging threat landscape. Moreover, data reveal major unawareness in the type of cyberinsurance that enterprises carry, which may result in inflated confidence by senior leadership about what these policies cover. Finally, this year's survey results affirm that the use of AI in security operations is still novel; however, the involvement of security professionals in the development, onboarding, and implementation of AI is astonishingly low. Most concerning is the lack of involvement in the development of a policy that governs the use of AI technology within respondent enterprises.

Acknowledgments

ISACA would like to recognize:

Board of Directors

John De Santis, Chair

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

Niel Harper, Vice-Chair

CISA, CRISC, CDPSE, CISSP, NACD.DC

Chief Information Security Officer and Data Protection Officer, Doodle, Former Chief Information Security Officer, United Nations Office for Project Services (UNOPS), Germany

Stephen Gilfus

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

Gabriela Hernandez-Cardoso

NACD.DC

Former President and CEO, GE Mexico, 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 Board Member, Malaysia

Jamie Norton

CISA, CISM, CGEIT, CIPM, CISSP

Partner, McGrathNicol, Australia

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, CSX-P, CDPSE

Chief Executive Officer, introSight Ltd., Israel

Pamela Nigro

ISACA Board Chair, 2022-2023

CISA, CGEIT, CRISC, CDPSE, CRMA

Vice President, Security, Medecision, USA

Tracey Dedrick

ISACA Board Chair, 2020-2021

Former Executive Vice President and Head of Enterprise Risk Management, Santander Holdings, USA

Brennan P. Baybeck

ISACA Board Chair, 2019-2020

CISA, CISM, CRISC, CISSP

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

About ISACA

For more than 50 years, ISACA® (http://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 our DNA—our game-changing innovations are redefining the possibilities of digital experiences. We connect content and data and introduce new technologies that democratize creativity, shape the next generation of storytelling, and inspire entirely new categories of business.

RESERVATION OF RIGHTS

DISCLAIMER

ISACA has designed and created *State of Cybersecurity 2024: 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

X:
www.X.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAGlobal

Instagram:
www.instagram.com/isacanews/

Adobe

adobe.com/go/securitynews

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.