Omdia by informa techtarget

ISSA Information Systems Security Association International

The Life and Times of Cybersecurity Professionals, Volume VIII

Melinda Marks | *Practice Director*

April 2026

This Omdia eBook was commissioned by ISSA and is distributed under license from Informa TechTarget, Inc.

Research objectives

The eighth annual *Life and Times of Cybersecurity Professionals* study continues to pinpoint many of the same issues as previous editions, underscoring persistent challenges such as rising cyberthreats, IT complexity, ubiquitous vulnerabilities, heavy workloads, and difficulties embedding cybersecurity into organizational processes and cultures. Beyond illustrating cybersecurity problems, this year's edition highlights specific areas where cybersecurity professionals suggest ways their organizations can alleviate the burdens on cybersecurity practitioners, including adopting AI technology, while simultaneously bolstering defenses and reducing risks.

To understand these trends and the potential implications, Omdia executed a survey of 380 IT and cybersecurity professionals at organizations across the globe from the Information Systems Security Association's (ISSA) member list. This serves as the eighth such research project, dating back to 2016. All references to previous research in this ebook can be found in *The Life and Times of Cybersecurity Professionals Volume VII*.

This study sought to:

- **Determine** the job satisfaction of cybersecurity professionals.
- **Assess** cybersecurity skill gaps and ways to address them.
- **Examine** the benefits and challenges of careers in the cybersecurity industry.
- **Recommend** ways to improve security careers and retain cybersecurity talent.

Note: Totals in figures and tables throughout this eBook may not add up to 100% due to rounding or organizations choosing more than one answer to select questions.

Key findings

Certifications, training, and networking are helpful for cybersecurity careers

PAGE 4

Cybersecurity professionals face job stress but feel rewarded by compensation

PAGE 7

Business alignment and collaboration across teams are important for cybersecurity culture

PAGE 13

As skill gap challenges persist, AI may be a force multiplier for security

PAGE 16

CISO roles are evolving with virtual CISOs and the need for leadership and business skills over technical skill

PAGE 20

Back to Contents


Certifications, training, and networking are helpful for cybersecurity careers

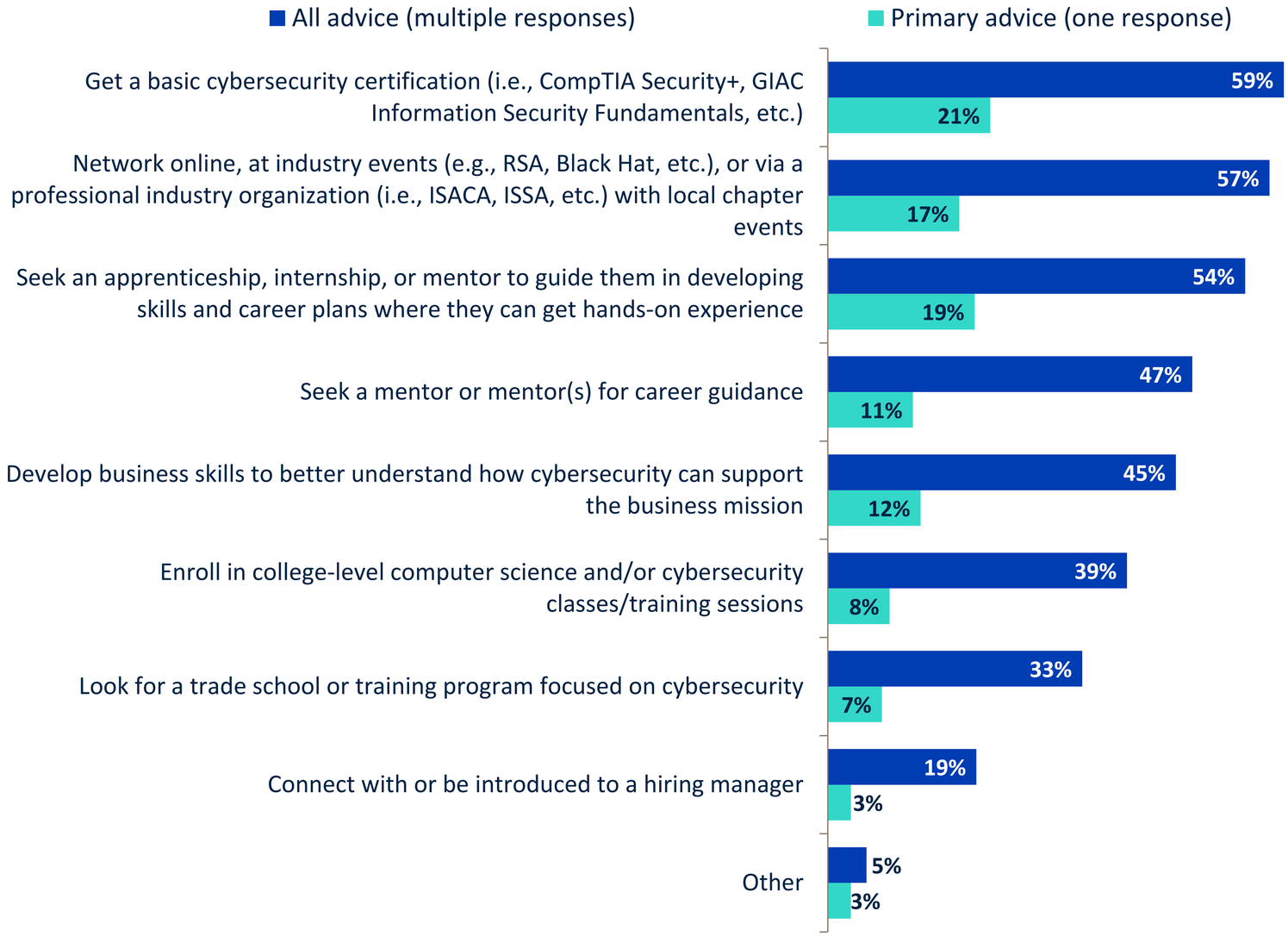
Career advice for joining cybersecurity

ISSA members offer advice across several areas to help others get into the cybersecurity field. The top three ways:

1. Get basic certifications.
2. Network online, at events, or via a professional organization.
3. Seek an apprenticeship, internship, or mentor.

Compared with past years, online networking has risen in importance. Also, cybersecurity professionals are increasingly recommending developing business skills to better understand how cybersecurity can support the business mission. This is valuable advice for those interested in joining the industry.

Advice cybersecurity professionals would give to people who want to get into the cybersecurity field.



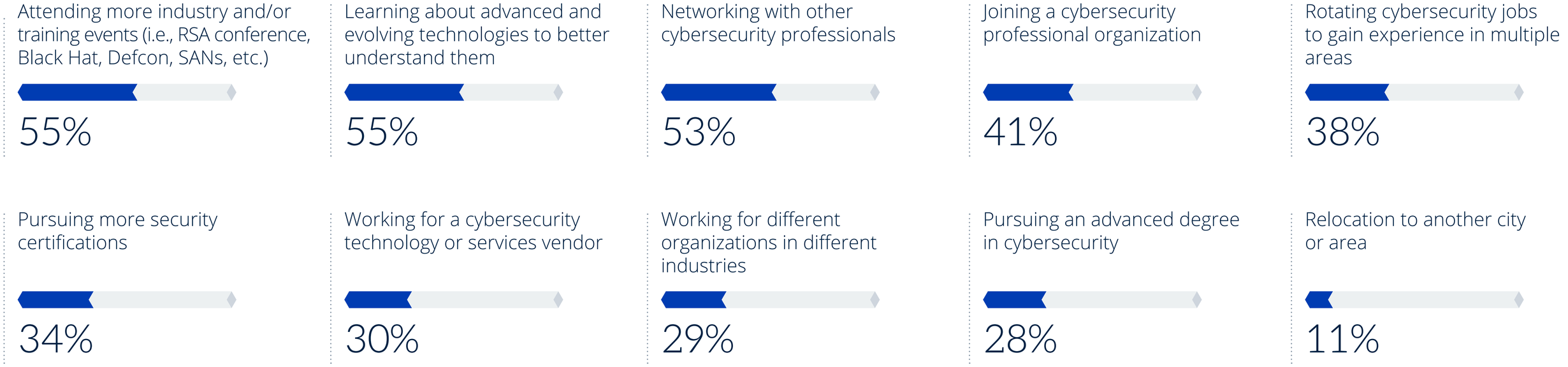
Back to Contents

Helpful career advancement actions

Respondents also shared what would be the most helpful actions for career advancement. The top include attending industry events, learning about advanced and evolving technologies, and networking.

Staying educated about new technologies is especially important with the rapid evolution of innovative tools, including AI. Effectiveness in the profession requires staying up to date on techniques and cutting-edge technologies that can help professionals and their team members stay ahead of the latest threats and attacks.

Most helpful actions for the advancement of cybersecurity careers.



Back to Contents

Cybersecurity professionals face job stress but feel rewarded by compensation

Cybersecurity is increasingly difficult

More than two-thirds (68%) of respondents indicated that being a cybersecurity professional has become more difficult over the past two years. Those who said working as a cybersecurity professional is more difficult today than it was two years ago cited a number of challenges underlying this belief. More than half (55%) cited the increase in cybersecurity complexity and workloads, and 52% cited cyberthreats and attack surface growth. Additionally, budgets, lack of investment in training, regulatory compliance challenges, and staffing issues were commonly identified as factors.

The current state of working as a cybersecurity professional.

26%

Working as a cybersecurity professional is **much more** difficult today than it was two years ago

42%

Working as a cybersecurity professional is **somewhat more** difficult today than it was two years ago

Why working as a cybersecurity professional is more difficult today than it was two years ago.

55%

Cybersecurity complexity and workload has increased

52%

Cyberthreats to my organization have increased as the attack surface has grown

36%

Cybersecurity budget pressures

35%

Lack of investment in advanced training for cybersecurity professionals

34%

Regulatory compliance has become more complex

33%

My organization's cybersecurity team is understaffed

25%

My organization lacks some cybersecurity awareness

16%

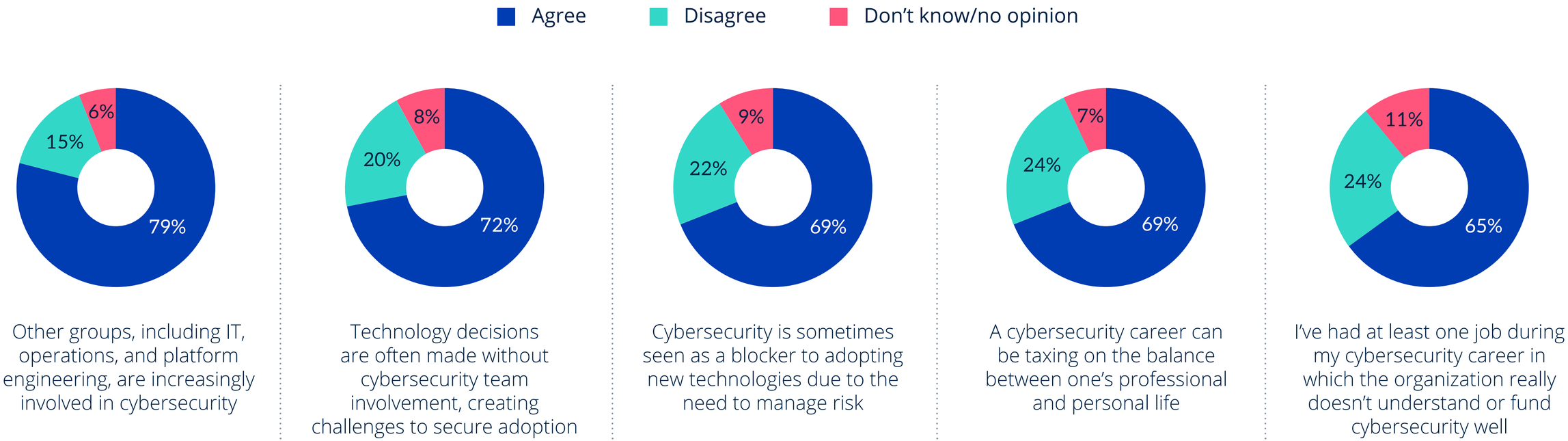
There is more cybersecurity oversight by executives and/or the board of directors

Back to Contents

Challenges faced by cybersecurity professionals

Respondents identified challenges caused by other groups' involvement in cybersecurity, as well as frustration when security is seen as an impediment to adopting new technologies. They also face challenges as their careers can be taxing on work/life balance, and it can be challenging if their cybersecurity program is not well understood or well-funded. These are key areas to address to improve cybersecurity job satisfaction.

Sentiments about the cybersecurity profession.



Back to Contents

Nearly all respondents report facing stressful aspects of their jobs

When asked about the most stressful aspects of a cybersecurity career, respondents identified a variety of factors generally related to people, process, and technologies contributing to stress. The top stressors included overwhelming workloads, keeping up with security for new IT initiatives, such as AI, fear of getting something wrong, and the pressure of emergencies or disruptions. Only 2% said they do not feel stressed about their jobs.

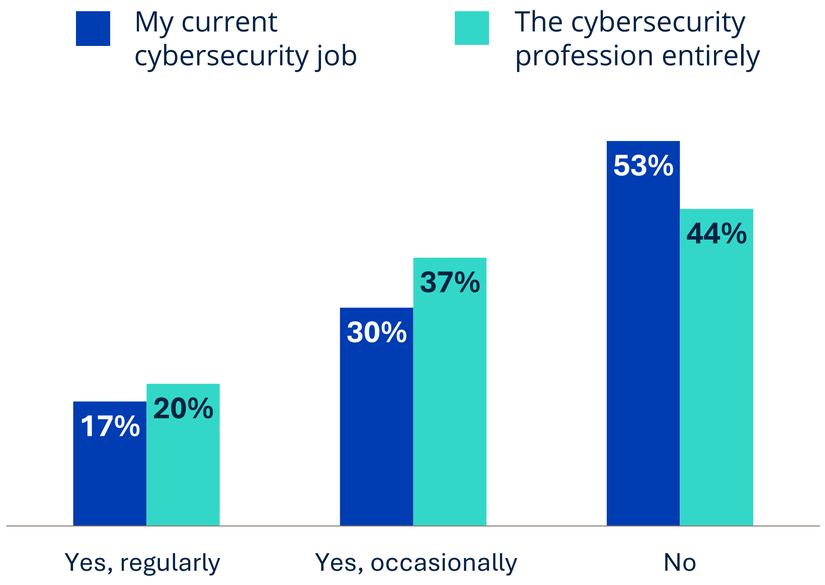
Most stressful aspects of a job or career as a cybersecurity professional.

Back to Contents

Reducing stress could prevent a cybersecurity exodus

Nearly half of respondents have occasionally (30%) or regularly (17%) thought about leaving their jobs over the last 12 to 18 months, and among those thinking of leaving their jobs, more than half have occasionally (37%) or regularly (20%) considered leaving the cybersecurity profession altogether. When asked for reasons behind their contemplation of leaving the cybersecurity profession, job stress is at the top of the list, followed by other challenges, such as chances for career advancement, work/life balance, and organizational commitment to cybersecurity.

Have respondents considered leaving their current job or the cybersecurity profession over the last 12 to 18 months?



Reasons for considering leaving the cybersecurity profession.

53%
High stress associated with a cybersecurity career

37%
No clear advancement opportunities

34%
A cybersecurity career does not provide a good work/life balance

33%
Lack of leadership commitment to cybersecurity in an organization

30%
I am close to retirement age and will leave the cybersecurity profession when I retire

29%
A cybersecurity career doesn't offer equitable compensation for the workload

Back to Contents

Cybersecurity job satisfaction can be fostered through culture and compensation

Cybersecurity professionals reported key aspects driving their job satisfaction. The three cited most commonly include having a leadership team committed to strong cybersecurity, receiving competitive compensation, and being offered support and financial incentives for staff to advance their careers. Respondents are also compensated in a variety of ways for meeting or exceeding performance goals. Specifically, the most common rewards include bonuses, professional training, and promotions. Interestingly, less than a quarter report getting raises for successful execution of duties. While bonuses are helpful, raises could also potentially help retain key cybersecurity professional talent.

Top five factors for determining level of job satisfaction.

How respondents are compensated for meeting or exceeding performance goals.

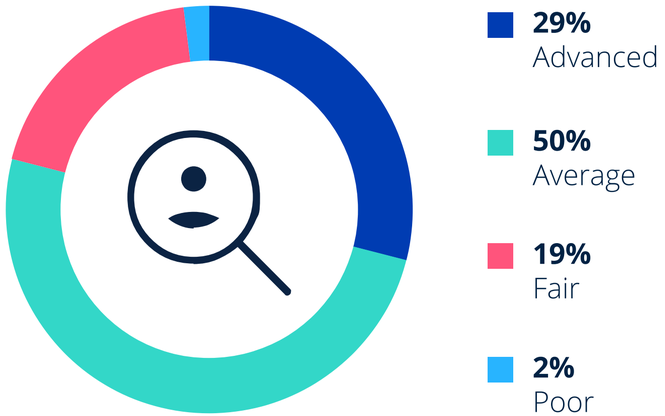
Back to Contents

Business alignment and collaboration across teams are important for cybersecurity culture

Professionals see multiple paths to improving cybersecurity culture

Only 29% of respondents rate their organization's cybersecurity culture as advanced, so there is much room for improvement. When it comes to improving cybersecurity culture, training cybersecurity and IT professionals tops the list of actions that make a difference. Investment in resources; improved governance, risk, and compliance; better cybersecurity hygiene; commitment to improving cybersecurity culture throughout the organization; and security awareness training are also important for building a strong cybersecurity culture.

How respondents characterize cybersecurity culture at their organization.



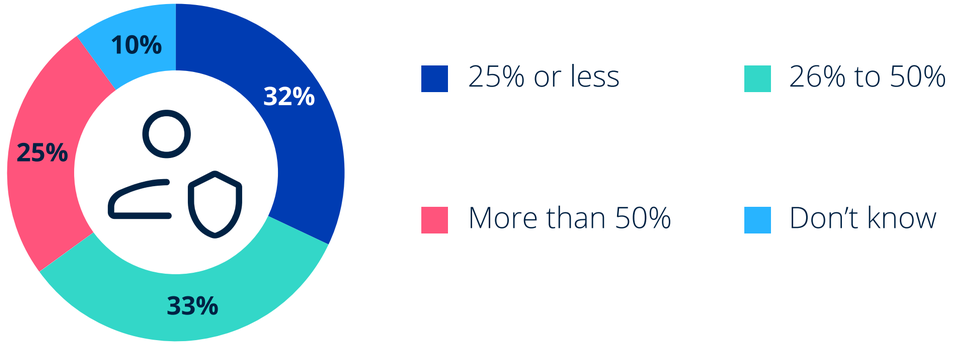
Actions respondents believe would improve their organization's cybersecurity program.

Back to Contents

Security must ensure collaboration with IT

IT staff spend high percentages of their time on cybersecurity tasks, so security excellence requires collaboration across teams. While the data shows heavy IT involvement in cybersecurity tasks, security needs to ensure it is involved to gain full visibility of security processes and tools as well as the status of activities. This requires close collaboration, embedding security into functional technology groups, automating processes, ensuring security oversight in IT projects, improving communication, and aligning on goals.

Percentage of day-to-day cybersecurity tasks done by people with IT (rather than cybersecurity) titles.



Most impactful actions for improving the working relationship between cybersecurity and IT teams.

44%

Embed cybersecurity staff members into functional technology groups

41%

Automate processes that require collaboration between IT and security teams

38%

Build appropriate information security oversight in IT projects where applicable

34%

Improve communications between cybersecurity and IT staff

29%

Alter employee compensation so that security and IT teams are rewarded to achieve common goals and objectives

25%

Standardize on common data sets and tools that can be used across security and IT

22%

Adopt a DevSecOps model

Back to Contents

As skill gap challenges persist, AI may be a force multiplier for security

The impacts of cybersecurity skill shortage are significant

Three-quarters of respondents indicated that their organization has been impacted to some extent by the cybersecurity skill shortage. This is higher than in previous years. While the study didn't reveal that the cybersecurity skill shortage has gotten worse than in previous years, respondents reported significant impacts to their security programs, including redirected time, increased workload, factors contributing to "burn out" and stress, increased errors, and the need for more budget for services or consultants.

Have organizations been impacted by the global cybersecurity skill shortage?

It has **significantly** impacted our organization

It has **somewhat** impacted our organization

Type of impacts the cybersecurity skill shortage has had on organizations.

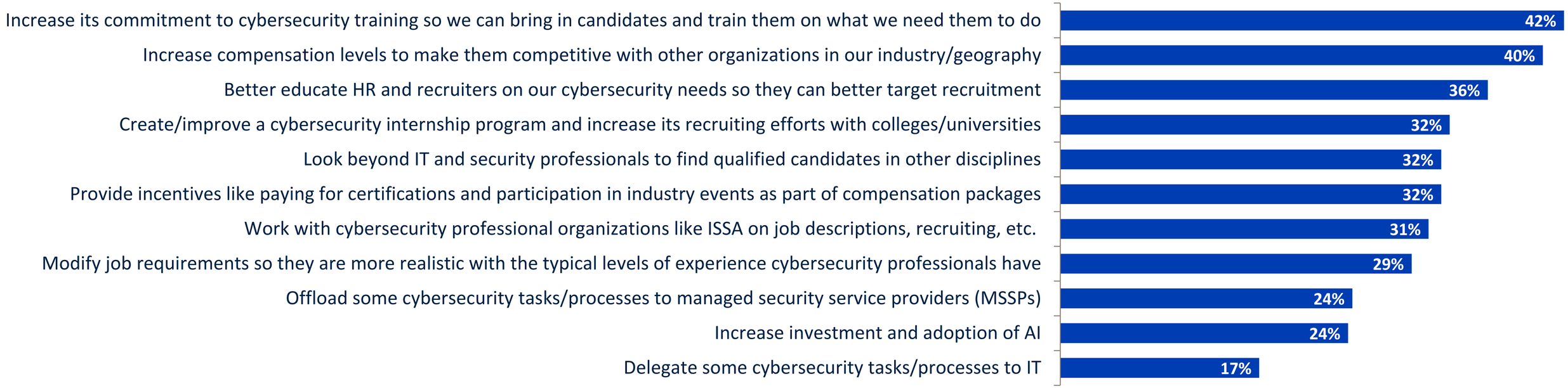
Back to Contents

Professionals have many ideas for addressing the impact of the cybersecurity skill shortage

Cybersecurity professionals seek multiple ways to address the impacts of the skill shortage, including increasing organizational commitment to cybersecurity, increasing compensation levels, and better education of HR and recruiters to target talent. The recommendations also often require industry collaboration, including setting up internship and mentorship programs, incentives for certifications, and working with professional organizations.

The lowest on the list: increasing investment and adoption of AI (24%) and delegating cybersecurity tasks and processes to IT (17%).

Actions organizations could take to address the impact of the cybersecurity skill shortage.

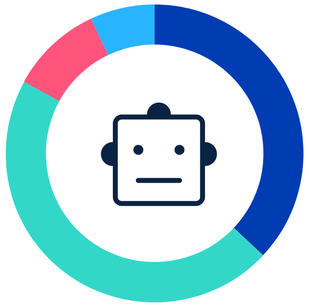


Back to Contents

Cybersecurity utilization of AI solutions

Although it wasn't high on the list of how cybersecurity professionals want to address the cybersecurity skill gap, utilizing AI may be helpful in alleviating the heavy workloads of cybersecurity professionals. For example, it can help automate tedious, time-consuming tasks, including data gathering and analysis. It could also help with speeding response time and simplifying remediation. As a result, most are using (37%) or planning to use (46%) AI solutions. Currently, half of organizations are using them to automate scanning and testing, with 48% leveraging the technology for predictive analysis, making these the two most commonly cited use cases.

Organizational position on utilizing AI solutions to solve cybersecurity issues.



37%
We are currently utilizing AI solutions

46%
We are considering utilizing AI solutions in the near future

10%
We are not utilizing or considering AI solutions at this time

Areas of cybersecurity for which organizations are utilizing or looking to utilize AI solutions.

50% Automating assessments, scanning, or testing of software

48% Predictive analysis (i.e., risk scoring for proactive remediation recommendations)

38% Threat/malware detection

37% Network and security management

35% Automating software remediation of security vulnerabilities

32% Incident response

26% AI-enabled authentication

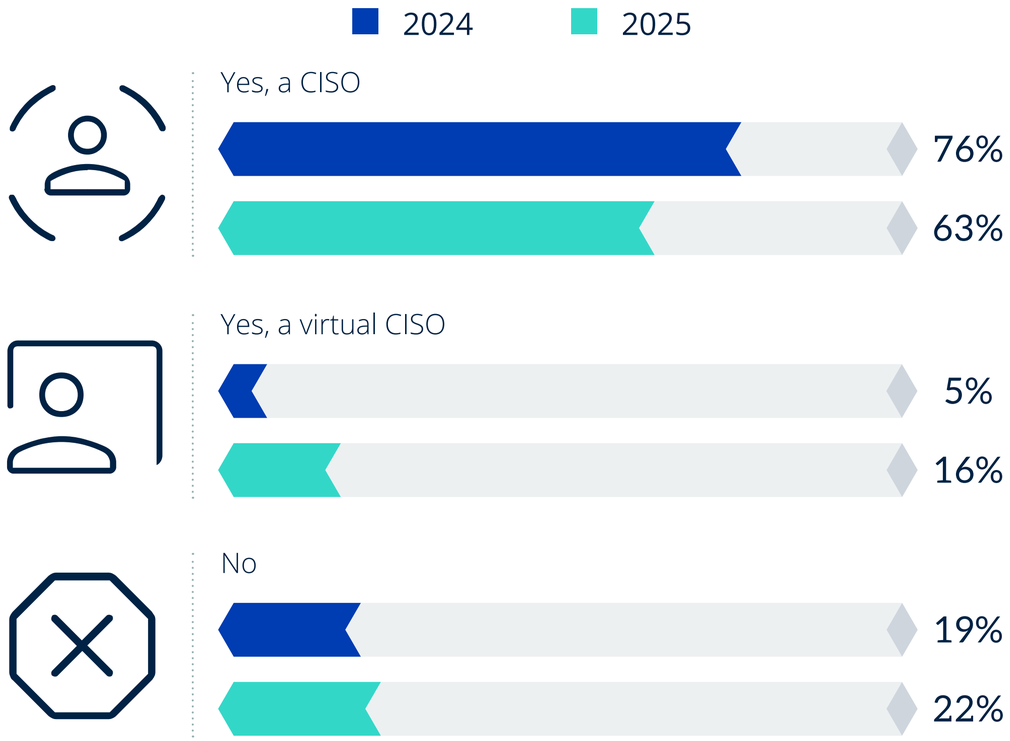
Back to Contents

CISO roles are evolving with virtual CISOs and the need for leadership and business skills over technical skill

Teams see a reduced number of CISOs with increasing virtual CISOs

Nearly two-thirds (63%) of organizations have CISOs, which is less than was reported in 2024. However, there was a noticeable jump in the number of virtual CISOs. Organizations are hiring virtual CISOs if the size of the organization does not warrant the expense of a full-time CISO, if the organization is exploring whether they need a full-time CISO, if they feel like they only need an experienced advisor, or if the organization is between full-time CISOs.

Do organizations have a CISO in place today?



Why organizations have a virtual CISO.

48% Size of the organization does not warrant the expense of a full-time CISO

40% Exploring whether the organization needs a full-time CISO role

37% Used as an experienced advisor only

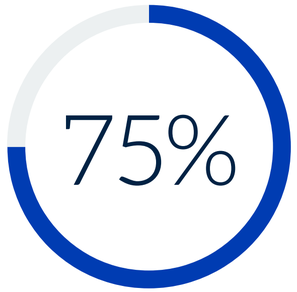
28% The organization is in between full-time CISOs

Back to Contents

CISOs most commonly report to IT

Similar to findings in past years' research, CISOs most often report into IT, although they may report into the CEO (27%) or COO (14%), and a small percentage (9%) report to the board of directors. Regardless of reporting structures, 75% of respondents regularly meet with executive management and the board of directors or a similar oversight group, underscoring the importance of cybersecurity to the business.

Do organizations' CISOs regularly meet with executive management and the board of directors?



Yes

No

Reporting structure for CISO/vCISO.

44%

CIO or another senior IT person

27%

CEO

14%

COO

9%

Board of directors

2%

Other

Back to Contents

Leadership and business and skills are important for successful CISOs

It is no surprise that the majority of respondents rate leadership (37%) or business (22%) skills as more important than those of a technical or operational nature. In previous years, communication skills were more often picked as the most important skill.

Most important quality of a successful CISO.

37%

Leadership skills

22%

Business skills

13%

Technical skills

13%

Management skills

10%

Operational skills

6%

Communications skills

Back to Contents

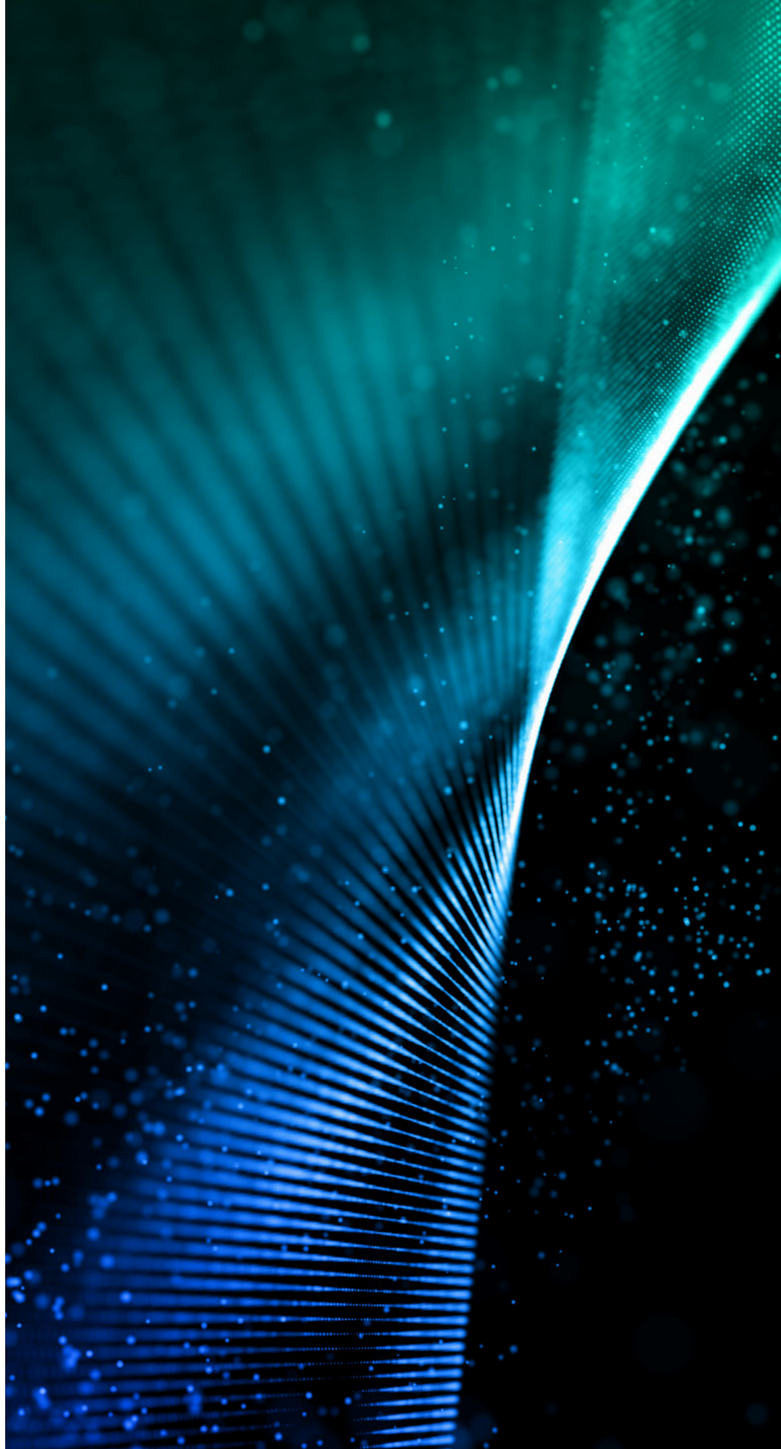
ISSA
Information Systems Security Association International

About

For four decades, ISSA has been the professional community where cybersecurity practitioners come to learn, connect, and grow, a member-driven organization that has stayed focused on the people doing this work and giving them the resources, knowledge, and community they need to do it well. ISSA is where cybersecurity professionals at every stage of their career find peers who understand the pressure, mentors who have navigated the same decisions, and a global network of chapters, events, and resources built around their development. Every year, ISSA members are the foundation of this research, sharing their honest experiences so the profession can see itself clearly and advocate for what it needs. What this study has shown consistently, across eight years, is that the practitioners who build sustainable careers in cybersecurity are rarely doing it alone. Fifty-five percent of cybersecurity professionals in this study say attending industry events advances their careers, and 41% say belonging to a professional organization does the same. If you are building a career in this field or working to make it sustainable for the long term, ISSA is where that work gets the support it deserves.

Learn More

Join ISSA



CSA cloud security alliance®

SANS

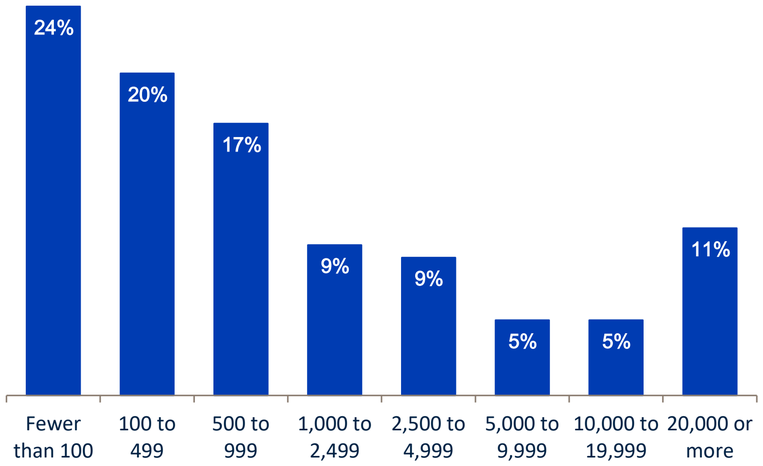
ISSA and Omdia would like to thank the Cloud Security Alliance and the SANS Institute for their support of this research initiative and their continued commitment to advancing the cybersecurity profession.

Research methodology and demographics

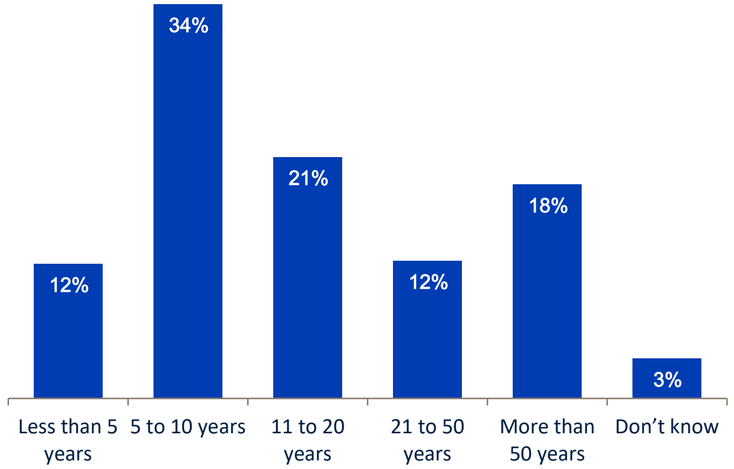
To gather data for this report, Omdia conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations across the globe between January 26, 2026, and February 18, 2026. To qualify for this survey, respondents were required to be members of ISSA's member list. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on several criteria) for data integrity, we were left with a final total sample of 380 IT and cybersecurity professionals.

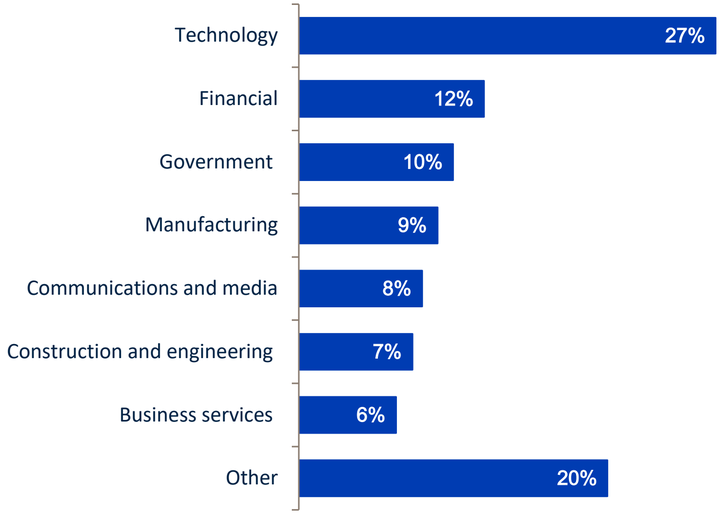
Respondents' organizations by number of employees.



Respondents' organizations by years in operation.



Respondents' organizations by industry.



Back to Contents

Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.