Enterprise Strategy Group™
by TechTarget

COMPLETE SURVEY RESULTS

The Life and Times of Cybersecurity Professionals

## *Volume VI, 2023*

Jon Oltsik | Distinguished Analyst and Fellow

About this Document

TechTarget's Enterprise Strategy Group (ESG)'s Complete Survey Results provide the complete output of syndicated research surveys in graphical format. In addition to the data, these documents provide background information on the survey, including respondent profiles at an individual and organizational level. It is important to note that these documents do not contain analysis of the data.

This Complete Survey Results presentation focuses on the experiences of cybersecurity professionals, including performance assessments of their cybersecurity leaders and their suggestions for what organizations can do to help cybersecurity professionals succeed.
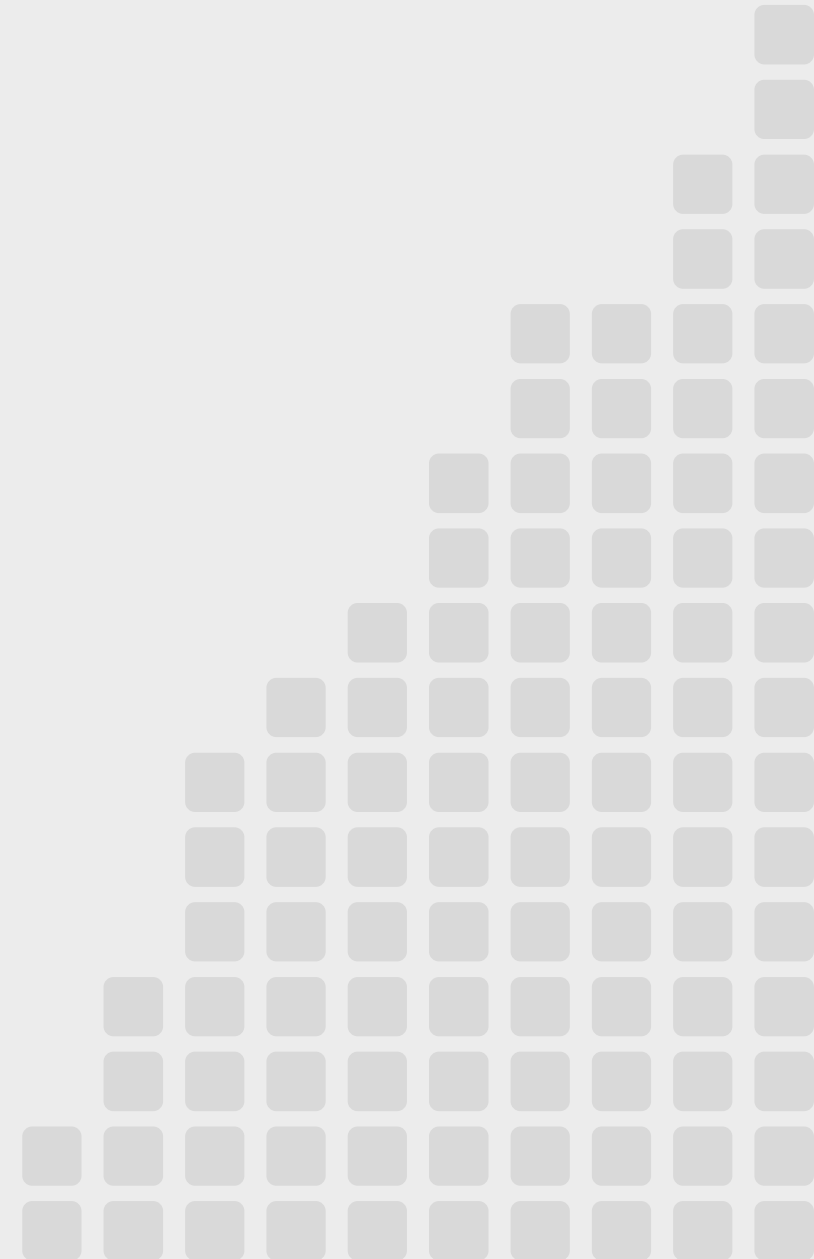
Research Objectives

- **Assess** the career progression of cybersecurity professionals.

- **Determine** whether cybersecurity professionals are satisfied with their careers and current jobs.

- **Measure** the impact of the global cybersecurity skills shortage and uncover what organizations are doing in response.

- **Monitor** cybersecurity leadership status.

Survey Details

QUANTITATIVE WEB-BASED SURVEY

- N=301 qualified completes.

- Global coverage (respondents from North America, Europe, Asia, Central/South America, and Africa).

- Field dates: 2/7/2023-3/12/2023.

SURVEY RESPONDENTS

- Information security and IT professionals from ISSA's member list.

- Employed at private- and pubic-sector organizations worldwide.

  - 39% midmarket or smaller (fewer than 1,000 employees).

  - 61% enterprise (1,000 or more employees).

- Multiple industry verticals including technology, government, financial, business services, and healthcare, among others.

- Complete demographics included at end of presentation.

Contents

- Survey Overview
- Research Methodology
- Research Data
  - Cybersecurity Career
  - Cybersecurity Career Satisfaction
  - Cybersecurity Culture
  - Cybersecurity Skills Shortage
  - Cybersecurity Leadership
  - Respondent Demographics/Firmographics

Research Methodology

ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America (United States and Canada), Europe, Asia, Central/South America, and Africa between February 7, 2023 and March 12, 2023. To qualify for this survey, respondents were required to be information security and IT professionals from the Information Systems Security Association (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 a number of criteria) for data integrity, we were left with a final total sample of 301 senior information security and IT professionals.

Please see the Respondent Demographics section at the end of this presentation for more information on these respondents and their organizations.

Note: Totals in figures and tables throughout this document may not add up to 100% due to rounding.

Cybersecurity Career

Enterprise Strategy Group™
by TechTarget

Respondents by Length of Career

Approximately how long have you been employed as a cybersecurity professional? (Percent of respondents, N=301)

Less than 1 year	1 to 3 years	4 to 6 years	7 to 10 years	11 to 15 years	16 to 20 years	More than 20 years
5%	11%	10%	18%	14%	13%	29%
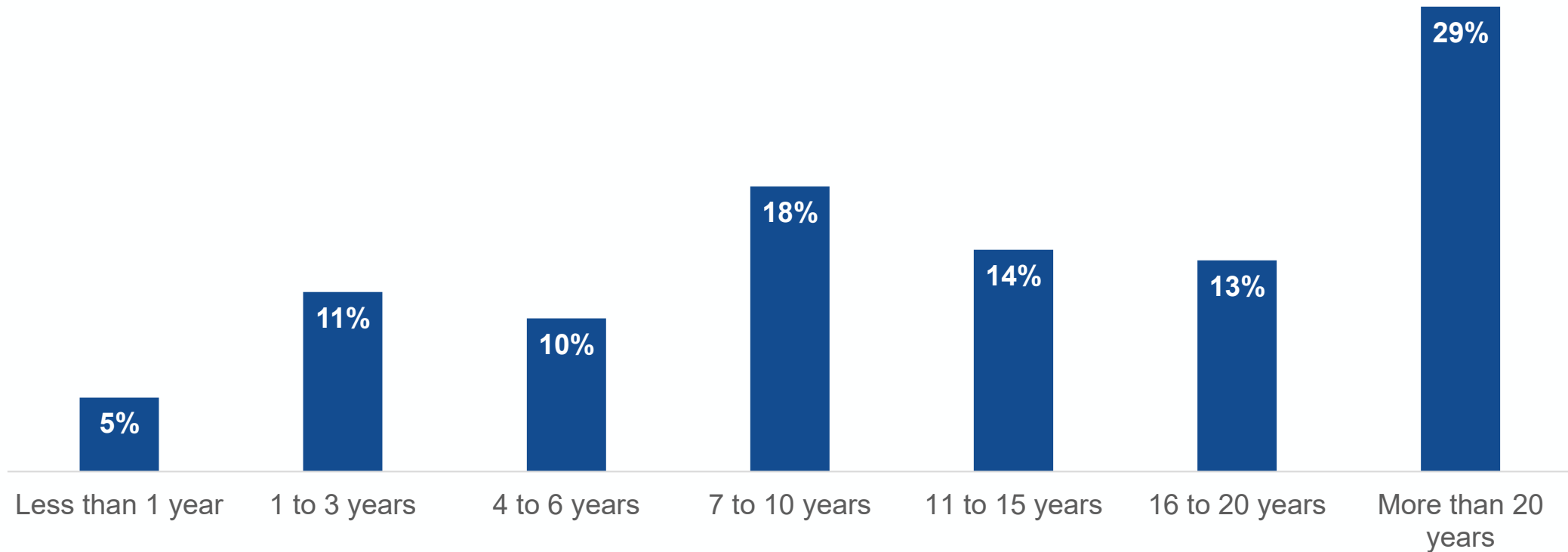
Total Number of Cybersecurity Jobs Spanning Career

Approximately how many different organizations have you worked for during the span of your cybersecurity career? (Percent of respondents, N=301)

Category	Percentage
1	17%
2	21%
3	17%
4	15%
5	9%
6	11%
More than 6	11%
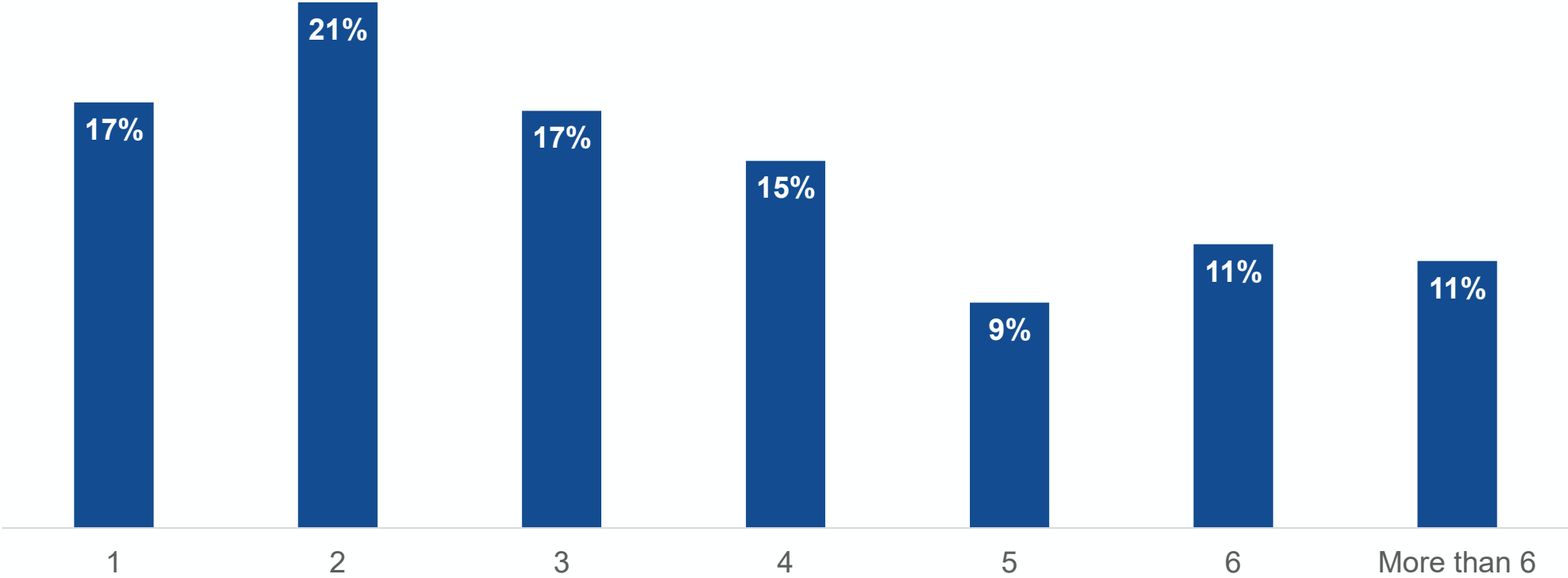
Cybersecurity Profession Is Getting More Difficult

Which of the following statements is most accurate based on your recent experience?
(Percent of respondents, N=287)

Working as a cybersecurity professional is much more difficult today than it was 2 years ago	Working as a cybersecurity professional is somewhat more difficult today than it was 2 years ago	Working as a cybersecurity professional is no more difficult today than it was 2 years ago	Working as a cybersecurity professional is somewhat easier today than it was 2 years ago	Working as a cybersecurity professional is much easier today than it was 2 years ago
27%	36%	28%	6%	3%

Reasons Profession Has Become More Difficult Include Increased Complexity and Attack Surfaces

You indicated that working as a cybersecurity professional is more difficult today than it was 2 years ago. Why do you believe this is so? (Percent of respondents, N=181, multiple responses accepted)

Reason	Percent
Cybersecurity complexity and workload has increased	81%
Cyber-threats to my organization have increased as the attack surface has grown	59%
My organization's cybersecurity team is understaffed	46%
Cybersecurity budget pressures have made working as a cybersecurity professional more difficult	43%
Regulatory compliance has become more complex	43%

Resources Cybersecurity Professionals Would Use for Job Searches

If you were looking for a new cybersecurity job, which of the following resources would you rely upon to find the right position? (Percent of respondents, N=301, multiple responses accepted)

Resource	Percent
Professional network (i.e., reaching out to past colleagues)	81%
Social networks/platforms (e.g., LinkedIn, Facebook, etc.)	64%
Recruiters	58%
Professional cybersecurity associations	58%
Networking (i.e., reaching out to people I don't know to try to find leads)	53%
Industry events	31%
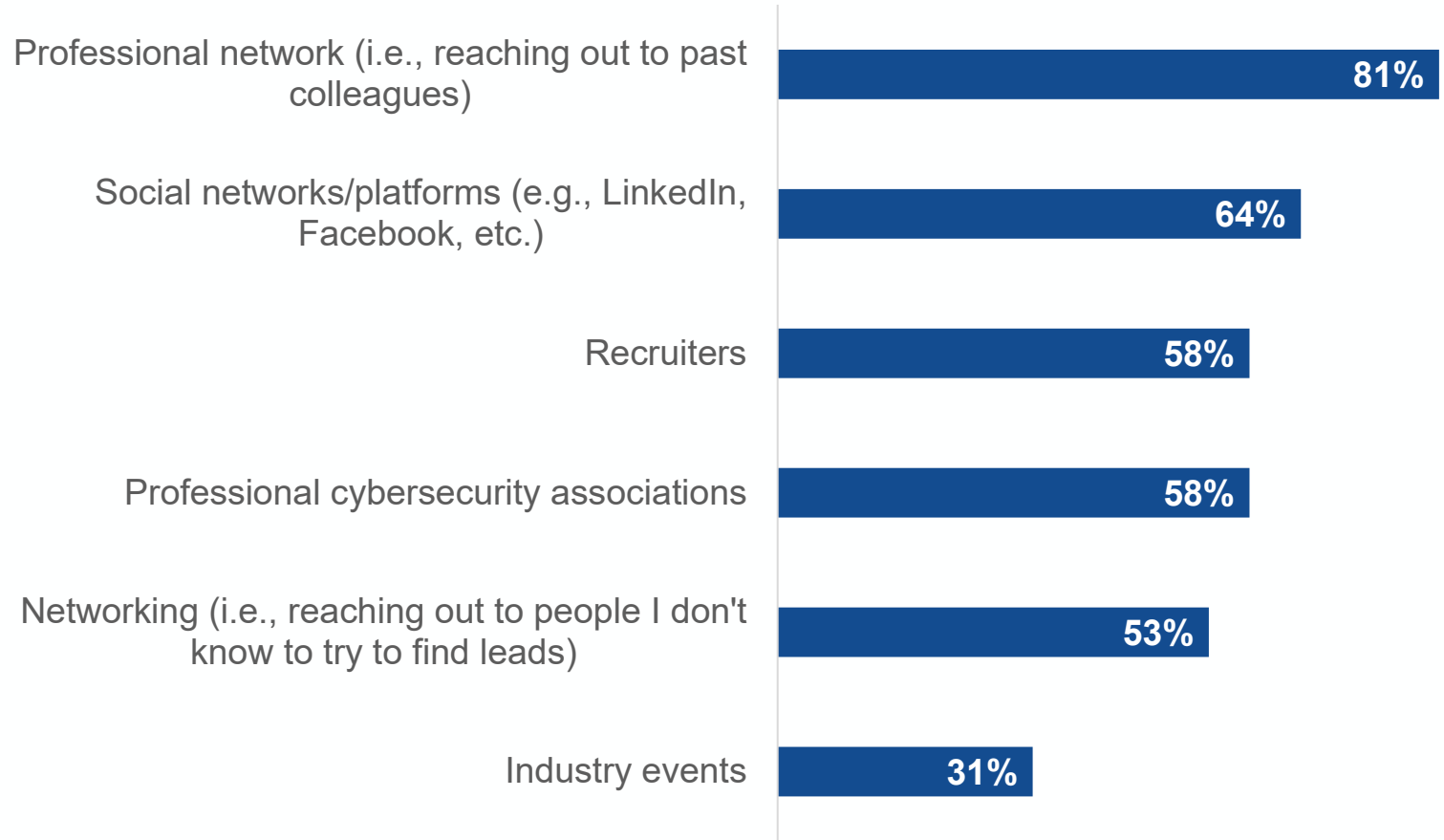
Career Advice for Prospective Cybersecurity Professionals

If you were advising someone who wanted to get into the cybersecurity field, what is the primary piece of advice you would give them? (Percent of respondents, N=301, one response accepted)

Advice	Percent
Seek an apprenticeship, internship, or mentor to guide them in developing skills and career plans where they can get hands-on experience	29%
Get a basic cybersecurity certification	27%
Network with or join a professional industry organization with local chapter events	15%
Enroll in college-level computer science and/or cybersecurity classes/training sessions	12%
Develop business skills to better understand how cybersecurity can support the business	11%
Develop soft skills	3%
Other	3%

Cybersecurity Certifications Achieved

Which of the following security certifications, if any, have you achieved? (Percent of respondents, N=301, multiple responses accepted)

Certification	Percent
Certified Information Systems Security Professional (CISSP)	52%
CompTIA Security+	29%
Certified Information Security Auditor (CISA)	20%
Certified Information Security Manager (CISM)	19%
CompTIA Network+	15%
Certified Ethical Hacker (CEH)	14%
Certified Cloud Security Specialist (CCSP)	12%
Cisco Certified Network Associate (CCNA)	12%
Certified in Risk and Information Systems Control (CRISC)	11%
GIAC Security Essentials Certification (GSEC)	7%
Certified CISO (CCISO)	7%
Systems Security Certified Practitioner (SSCP)	5%
Certified Incident Handler (GCIH)	5%
Certified in Governance of Enterprise IT (CGEIT)	5%
GIAC Certified Penetration Tester (GPEN)	1%
Cybersecurity Forensic Analyst (CSFA)	1%
I haven't received any security certifications	11%

Certifications With Measurable Career Impact

Of the security certifications you have achieved to date, which do believe has had a positive measurable impact on your career as a cybersecurity professional? (Percent of respondents, N=269, multiple responses accepted)

Certification	Percent
Certified Information Systems Security Professional (CISSP)	53%
CompTIA Security+	17%
Certified Information Security Auditor (CISA)	12%
Certified Information Security Manager (CISM)	11%
Certified in Risk and Information Systems Control (CRISC)	7%
Cisco Certified Network Associate (CCNA)	7%
Certified Ethical Hacker (CEH)	6%
Certified Cloud Security Specialist (CCSP)	5%
CompTIA Network+	5%
GIAC Security Essentials Certification (GSEC)	4%
Certified CISO (CCISO)	4%
Systems Security Certified Practitioner (SSCP)	3%
Certified Incident Handler (GCIH)	3%
Certified in Governance of Enterprise IT (CGEIT)	3%
Cybersecurity Forensic Analyst (CSFA)	1%
None of the above	5%

Cybersecurity Professionals' Opinions on Cybersecurity Landscape

Please select one response per row that best reflects your opinion on each statement. (Percent of respondents, N=301)

■ Agree ■ Neither agree nor disagree ■ Disagree ■ Don't know/no opinion

Statement	Agree	Neither agree nor disagree	Disagree	Don't know/no opinion
Cybersecurity professionals must keep up with their skills or the organizations they work for are at a significant disadvantage against today's cyber-adversaries	90%	7%	3%	
I've had at least one job during my cybersecurity career in which the organization really doesn't understand or fund cybersecurity well	69%	14%	16%	1%
A cybersecurity career can be taxing on the balance between one's professional and personal life	68%	21%	10%	1%
While I try to keep up on cybersecurity skills, it is hard to do so given the demands of my job	57%	19%	23%	1%
Cybersecurity professionals too often focus on new technology trends and not enough on how security aligns with the corporate mission	55%	29%	13%	2%

Cybersecurity Career Advancement Techniques

Which of the following actions do you believe would be the most helpful for you in the advancement of your cybersecurity career? (Percent of respondents, N=301, multiple responses accepted)
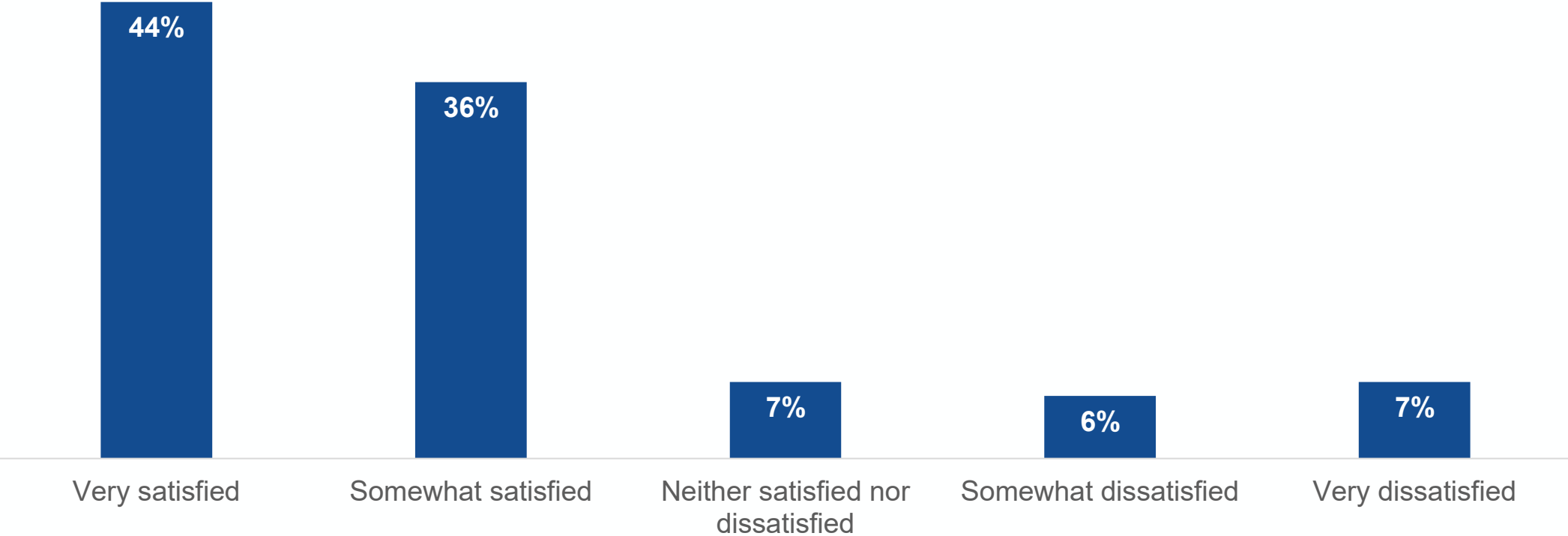
Action	Percent
Networking with other cybersecurity professionals	62%
Attending more training sessions	49%
Attending more industry events	47%
Joining a cybersecurity professional organization	45%
Rotating cybersecurity jobs to gain experience in multiple areas	42%
Pursuing more security certifications	42%
Working for different organizations in different industries	35%
Pursuing an advanced degree in cybersecurity	26%
Working for a cybersecurity services vendor	16%
Working for a cybersecurity technology vendor	15%

Cybersecurity Career Satisfaction

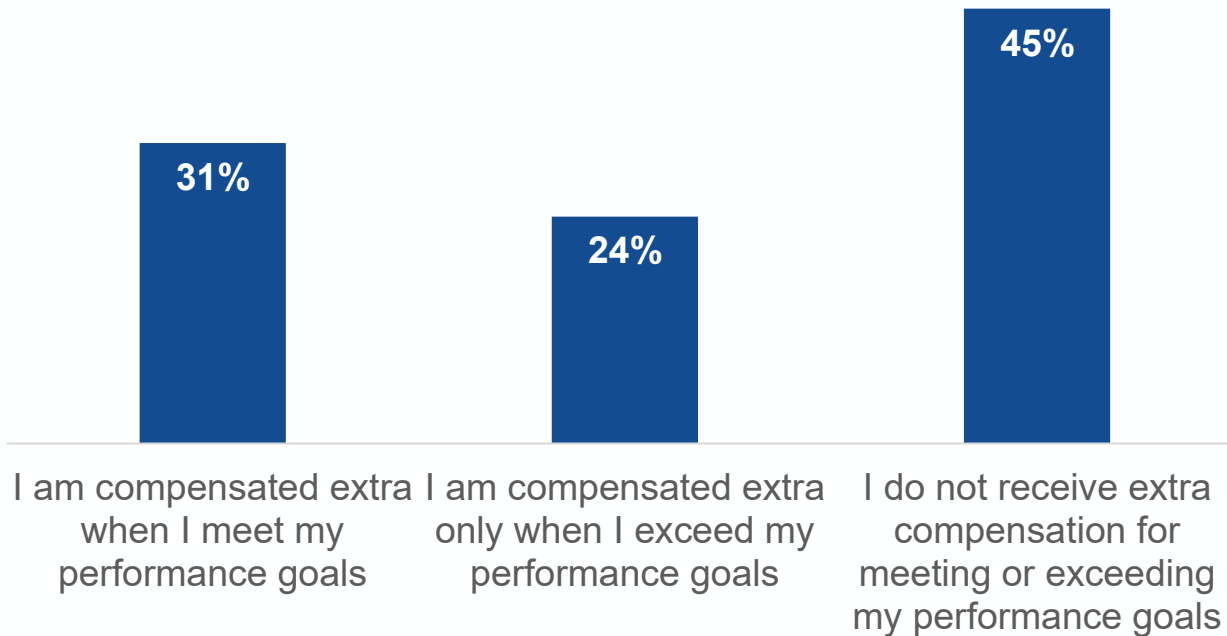Enterprise Strategy Group™
by TechTarget

Less than Half of Cybersecurity Professionals Are Very Satisfied With Their Current Jobs

How satisfied are you at your current job? (Percent of respondents, N=301)

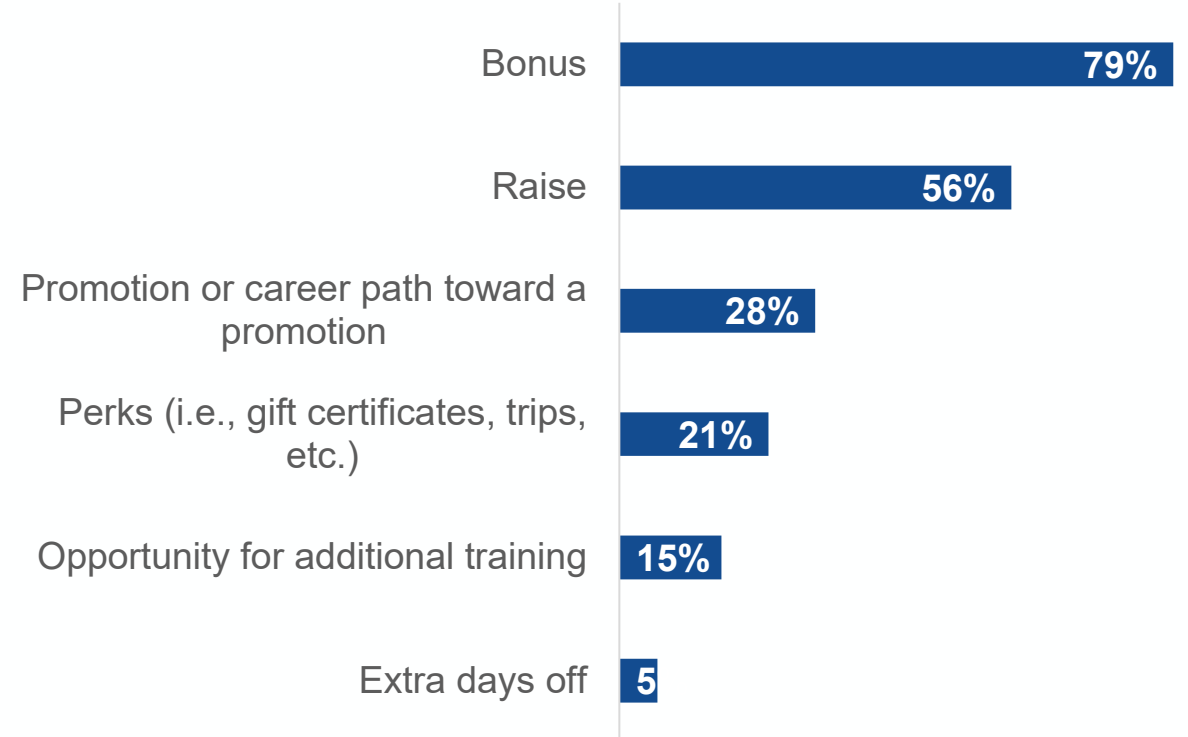| Very satisfied	Somewhat satisfied	Neither satisfied nor dissatisfied	Somewhat dissatisfied	Very dissatisfied
44%	36%	7%	6%	7%

Compensation for Meeting/Exceeding Goals Likelier to Be Monetary in Nature

Which of the following statements about the connection between your performance goals and extra compensation is most accurate? (Percent of respondents, N=301)

Statement	Percent
I am compensated extra when I meet my performance goals	31%
I am compensated extra only when I exceed my performance goals	24%
I do not receive extra compensation for meeting or exceeding my performance goals	45%

How does your organization compensate you for meeting or exceeding your performance goals? (Percent of respondents, N=165, multiple responses accepted)
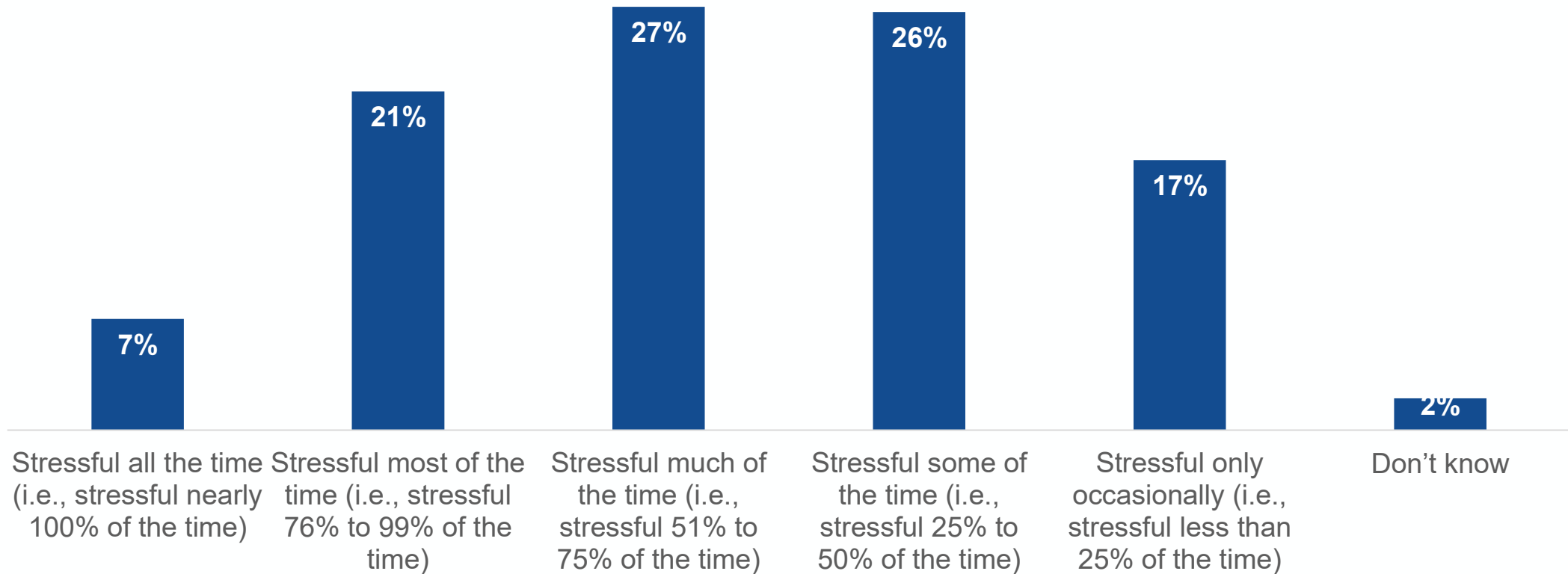
Method	Percent
Bonus	79%
Raise	56%
Promotion or career path toward a promotion	28%
Perks (i.e., gift certificates, trips, etc.)	21%
Opportunity for additional training	15%
Extra days off	5

Factors Determining Job Satisfaction Include Compensation and Business Commitment to Strong Cybersecurity

Which of the following are the biggest factors for determining your level of job satisfaction? (Percent of respondents, N=301, three responses accepted)
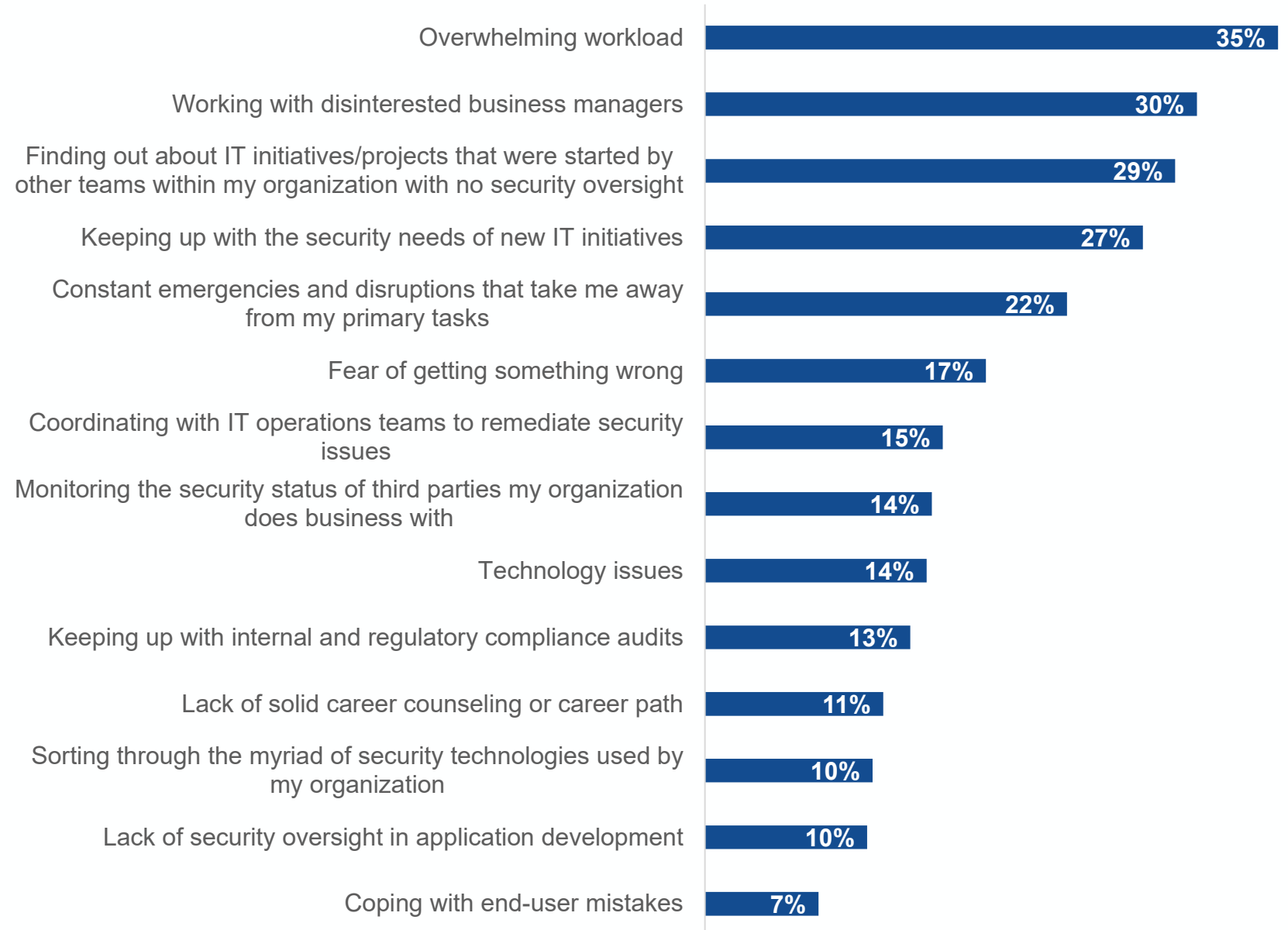
Factor	Percent
Competitive or industry-leading financial compensation	43%
Business management's commitment to strong cybersecurity	41%
The ability to work with a highly skilled and talented cybersecurity staff	38%
Organization provides support and financial incentives, enabling cybersecurity staff to advance their careers	36%
Organization provides opportunities for career advancements and promotions	25%
Strong leadership from the CISO and other security managers	24%
The ability to learn business processes and work closely with business units	20%
The ability to work with the latest types of IT and/or cybersecurity technologies	14%
Clear, concise, and consistent job descriptions and responsibilities that are agreed upon by business, IT, and security management	14%
Organization has a mentoring program where an employee can learn from more experienced peers	11%

Majority Say that a Cybersecurity Career Is Stressful at Least Half the Time

Generally speaking, which of the following statements most closely characterizes the stress level typically associated with your cybersecurity career? (Percent of respondents, N=301)


Stressful all the time (i.e., stressful nearly 100% of the time)	Stressful most of the time (i.e., stressful 76% to 99% of the time)	Stressful much of the time (i.e., stressful 51% to 75% of the time)	Stressful some of the time (i.e., stressful 25% to 50% of the time)	Stressful only occasionally (i.e., stressful less than 25% of the time)	Don't know
7%	21%	27%	26%	17%	2%

Stressful Aspects of the Cybersecurity Profession Include Workloads and Dealing with Business Managers

What are the most stressful aspects of your job/career as a cybersecurity professional? (Percent of respondents, N=301, three responses accepted)

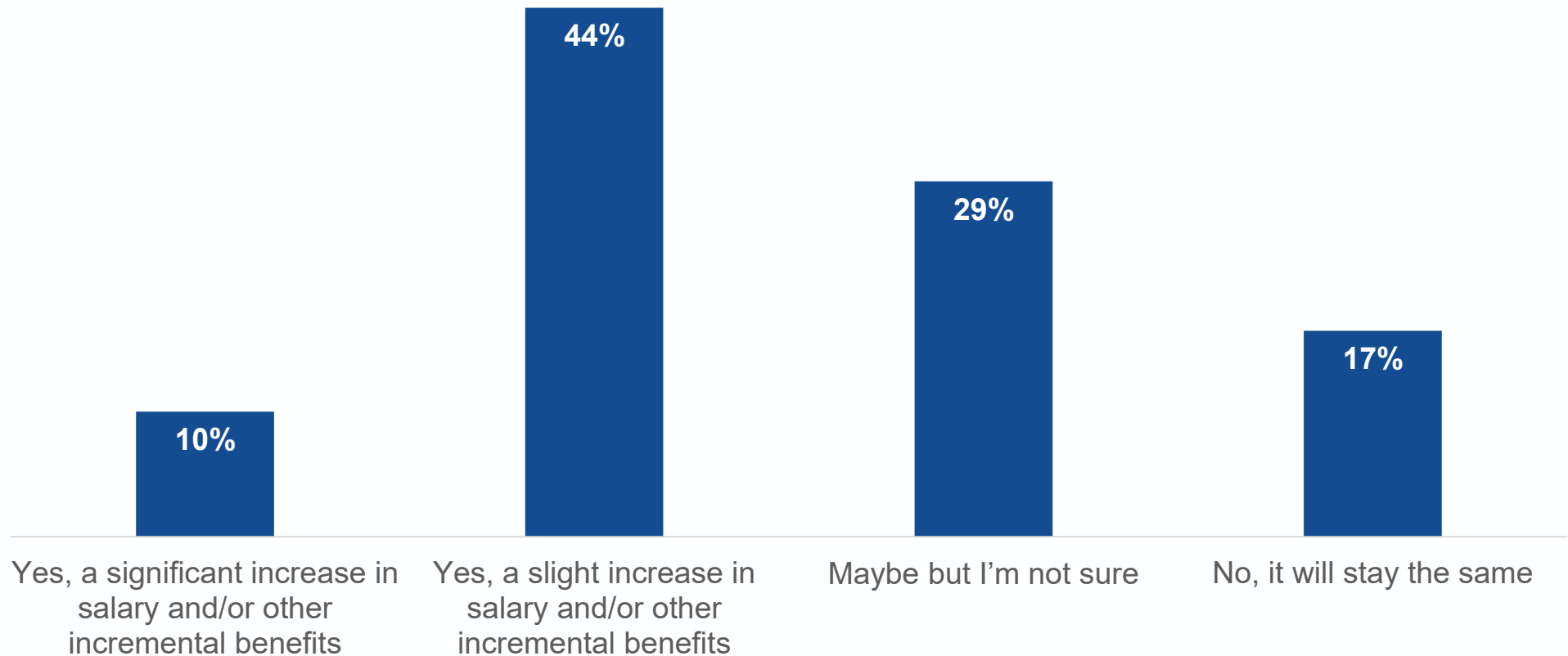| Aspect	Percent
Overwhelming workload	35%
Working with disinterested business managers	30%
Finding out about IT initiatives/projects that were started by other teams within my organization with no security oversight	29%
Keeping up with the security needs of new IT initiatives	27%
Constant emergencies and disruptions that take me away from my primary tasks	22%
Fear of getting something wrong	17%
Coordinating with IT operations teams to remediate security issues	15%
Monitoring the security status of third parties my organization does business with	14%
Technology issues	14%
Keeping up with internal and regulatory compliance audits	13%
Lack of solid career counseling or career path	11%
Sorting through the myriad of security technologies used by my organization	10%
Lack of security oversight in application development	10%
Coping with end-user mistakes	7%

Many Cybersecurity Pros Feel Underpaid to Some Extent

How do you believe your total compensation package compares with other security professionals with similar roles and responsibilities? (Percent of respondents, N=301)


6%	16%	38%	26%	14%
Significantly more than others with similar roles and responsibilities	Somewhat more than others with similar roles and responsibilities	About the same as others with similar roles and responsibilities	Somewhat less than others with similar roles and responsibilities	Significantly less than others with similar roles and responsibilities
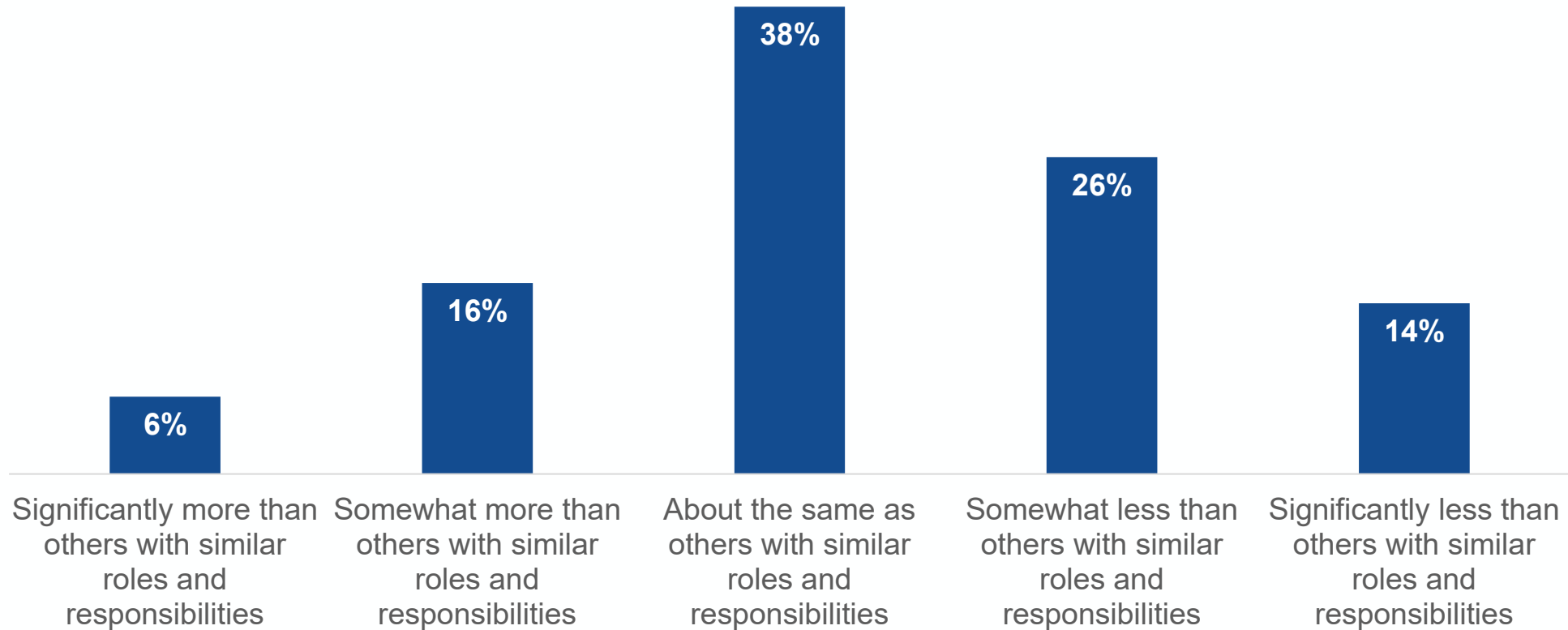
Most Cybersecurity Pros Expect a Salary Increase in 2023

Do you expect to receive an increase in salary or other incremental benefits from your current employer in 2023? (Percent of respondents, N=301)


- Yes, a significant increase in salary and/or other incremental benefits — **10%**
- Yes, a slight increase in salary and/or other incremental benefits — **44%**
- Maybe but I'm not sure — **29%**
- No, it will stay the same — **17%**

More than One-quarter of Cybersecurity Pros Likely to Leave Job in 2023 or Have Considered Leaving Cybersecurity Profession Entirely

How likely are you to leave your current job in 2023 for any reason (e.g., retire, change careers, leave for another cybersecurity job, etc.)? (Percent of respondents, N=301)
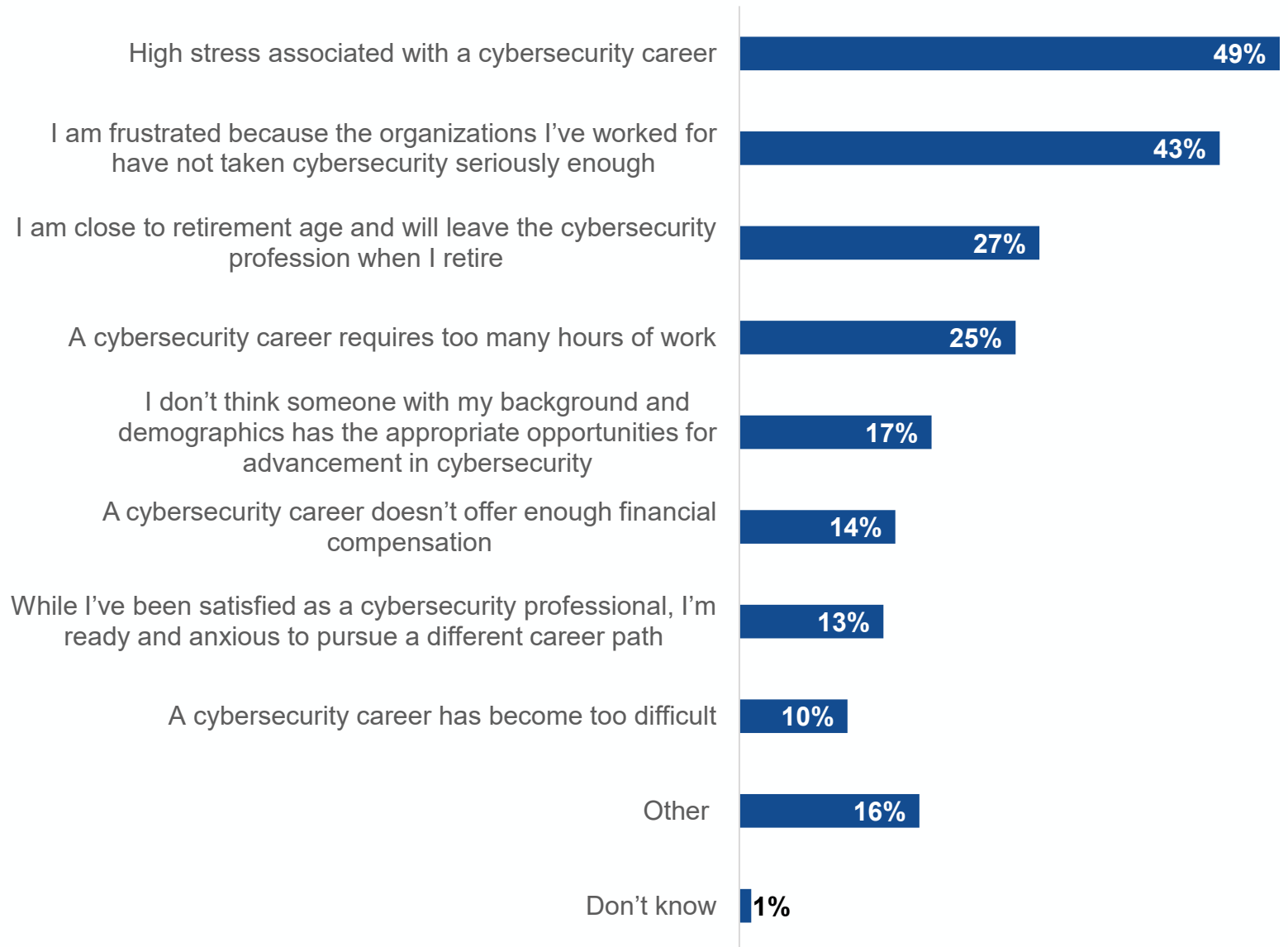

- Very likely: 21%
- Likely: 6%
- Somewhat likely: 23%
- Not at all likely: 43%
- Don't know: 8%
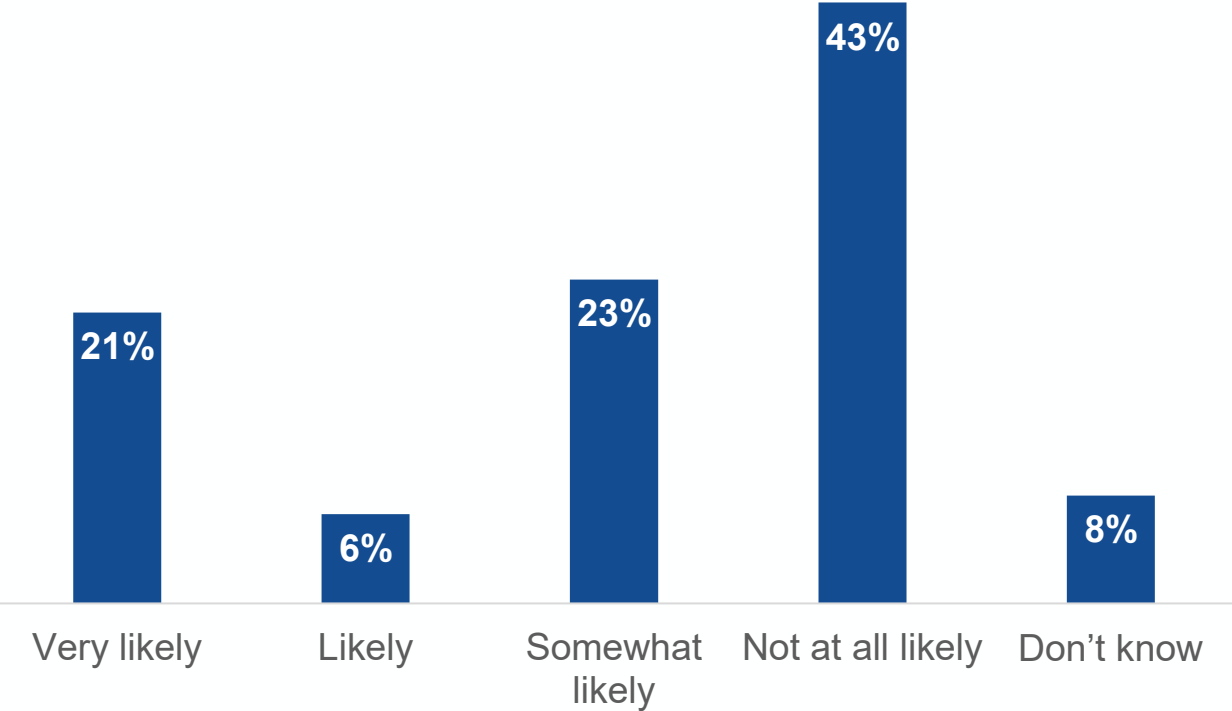
Have you considered leaving the cybersecurity profession over the last 12 to 18 months? (Percent of respondents, N=301)

- Yes, regularly, 9%
- Yes, occasionally, 21%
- No, 69%
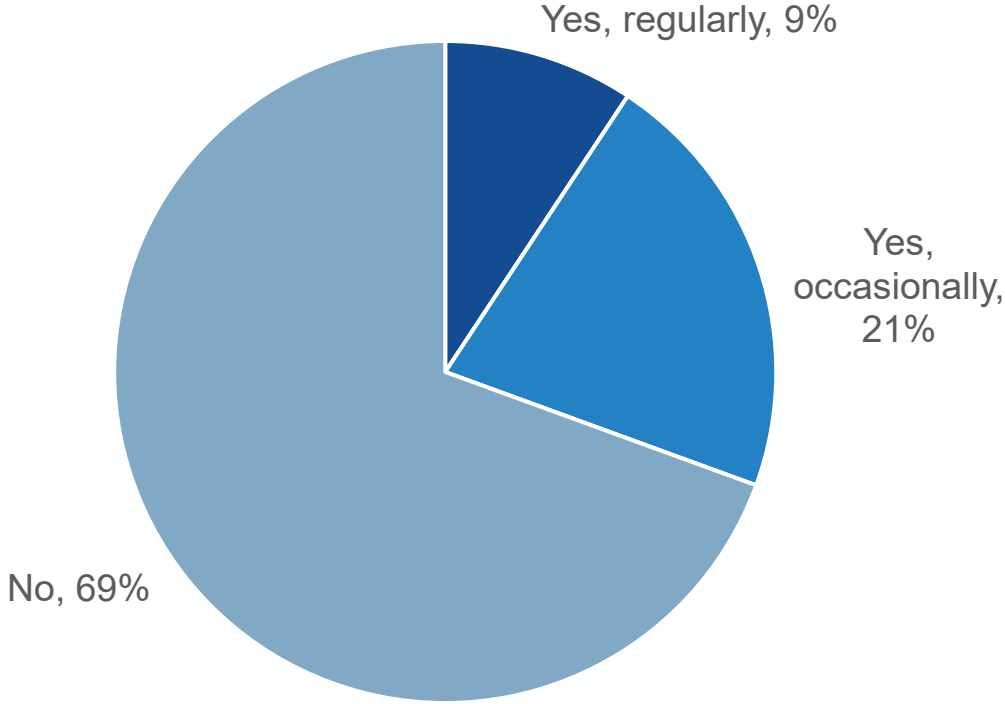
Stress and Underprioritizing Cybersecurity Most Common Reasons for Leaving the Profession

Which of the following are reasons you've considered leaving the cybersecurity profession over the last 12-18 months? (Percent of respondents, N=92, multiple responses accepted)

Reason	Percent
High stress associated with a cybersecurity career	49%
I am frustrated because the organizations I've worked for have not taken cybersecurity seriously enough	43%
I am close to retirement age and will leave the cybersecurity profession when I retire	27%
A cybersecurity career requires too many hours of work	25%
I don't think someone with my background and demographics has the appropriate opportunities for advancement in cybersecurity	17%
A cybersecurity career doesn't offer enough financial compensation	14%
While I've been satisfied as a cybersecurity professional, I'm ready and anxious to pursue a different career path	13%
A cybersecurity career has become too difficult	10%
Other	16%
Don't know	1%

Cybersecurity Culture

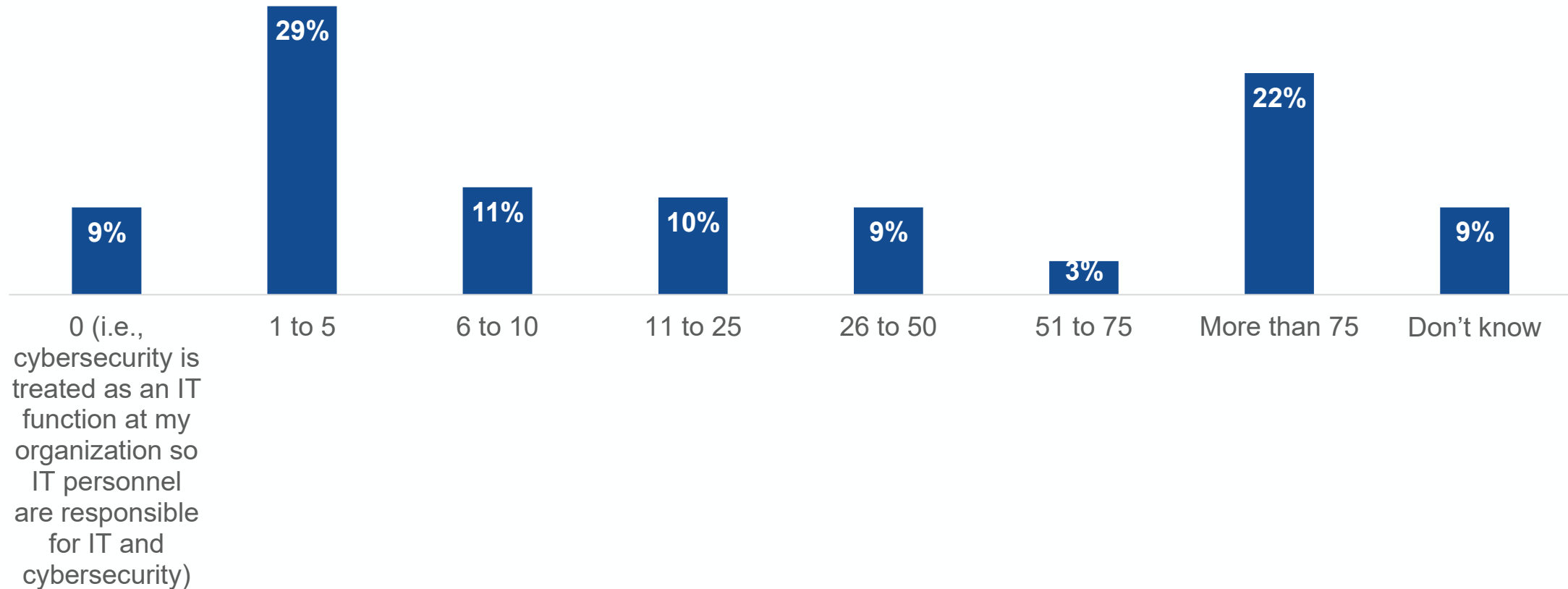Enterprise Strategy Group™
by TechTarget

More than Two-thirds Say Their Organization's Cybersecurity Culture Is Average at Best

How would you characterize the cybersecurity culture at your organization? (Percent of respondents, N=301)

31% — Advanced: Cybersecurity is considered a shared responsibility by all employees and is included in all business/mission initiatives

43% — Average: Cybersecurity is considered a shared responsibility by some employees and is included in some business/mission initiatives

20% — Fair: While my organization makes some efforts, cybersecurity is only partially considered a shared responsibility by employees and partially included in business/mission initiatives

7% — Poor: My organization makes little cybersecurity efforts, so cybersecurity is hardly considered a shared responsibility by employees and hardly included in business/mission initiatives

Number of Full-time Cybersecurity Employees

Approximately how many full-time employees does your organization have dedicated to cybersecurity (i.e., cybersecurity planning, operations, threat intelligence analysis, incident response, vulnerability management, etc.)? (Percent of respondents, N=301)

Category	Percent
0 (i.e., cybersecurity is treated as an IT function at my organization so IT personnel are responsible for IT and cybersecurity)	9%
1 to 5	29%
6 to 10	11%
11 to 25	10%
26 to 50	9%
51 to 75	3%
More than 75	22%
Don't know	9%

Majority Say IT Handles More than One-quarter of Daily Cybersecurity Tasks

In your opinion, how much of your organization's day-to-day security tasks are done by people with IT (rather than security) titles? (Percent of respondents, N=301)
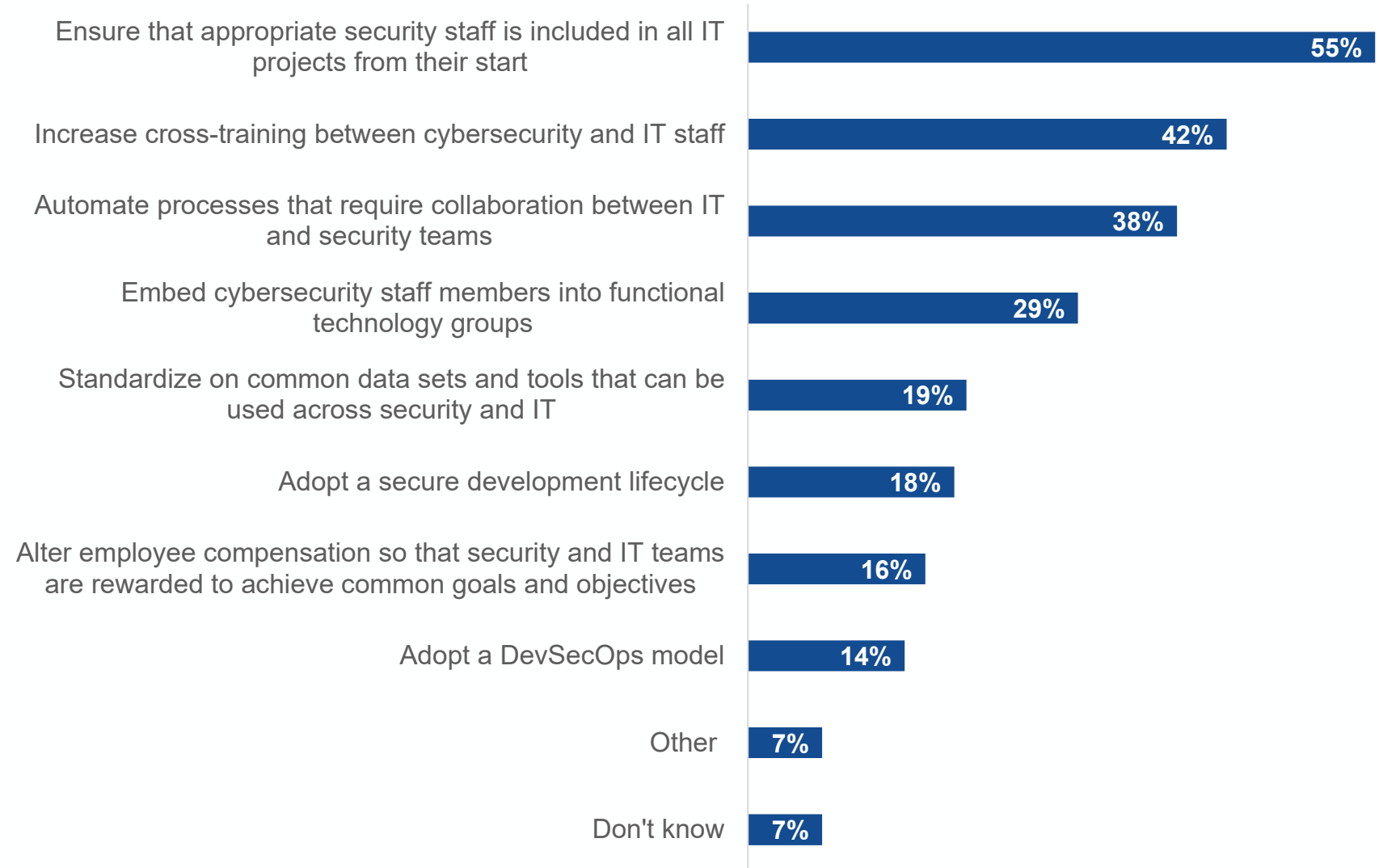

Less than 10%	10% to 25%	26% to 50%	51% to 75%	More than 75%	Don't know
21%	15%	22%	13%	16%	13%
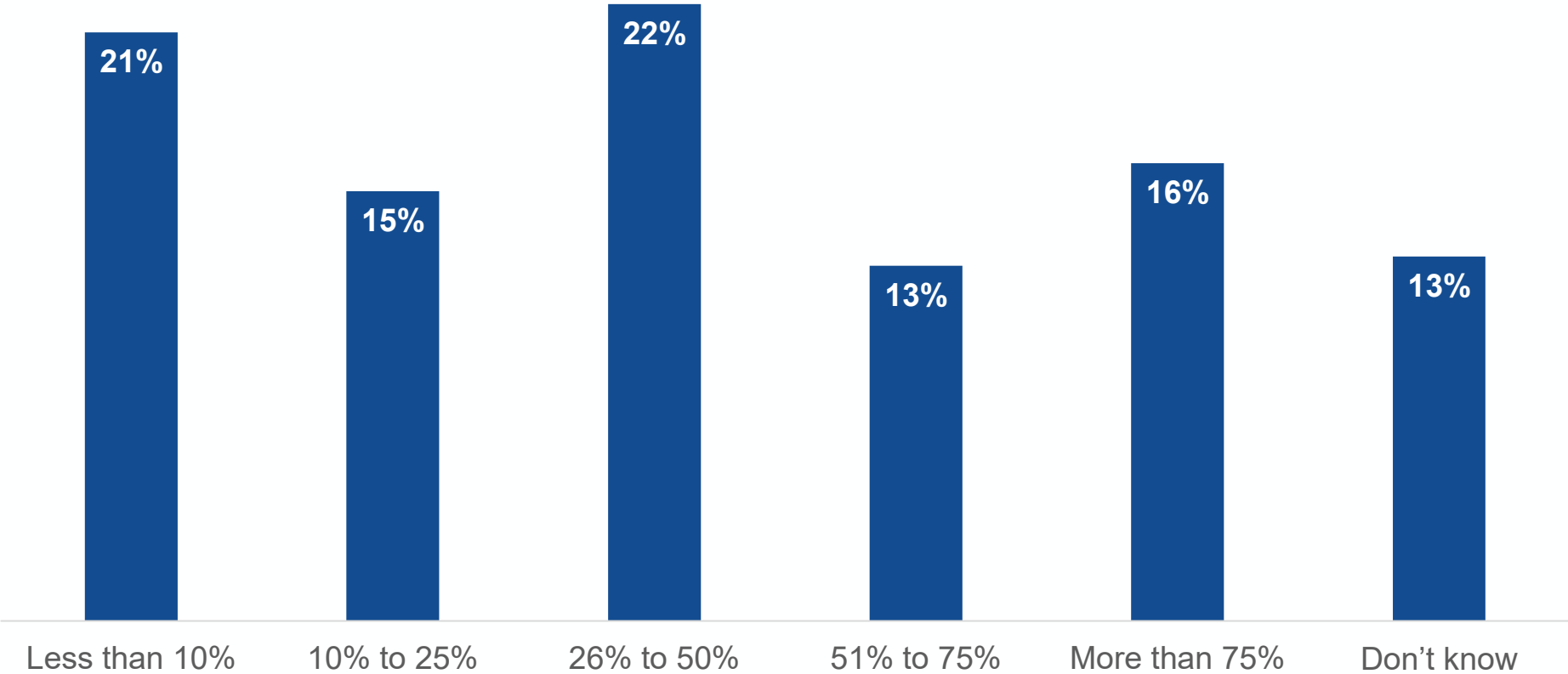
Cybersecurity Relationships Are Better with Technical Teams

How would you characterize the working relationship (i.e., communication, collaboration, common goals, and objectives, etc.) between your organization's cybersecurity department and each of these others? (Percent of respondents, N=301)
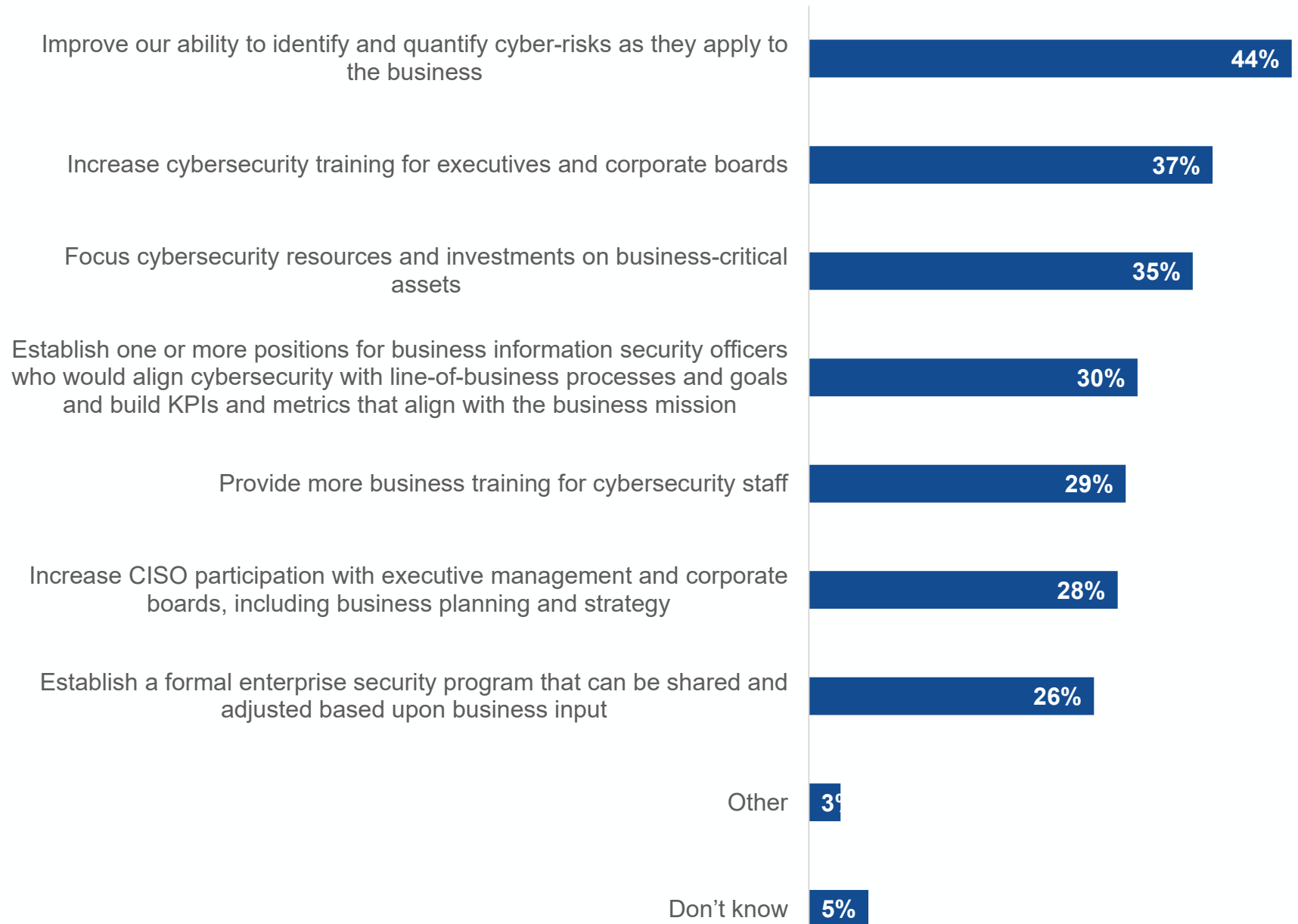
■ Very good   ■ Good   ■ Fair   ■ Poor

	Very good	Good	Fair	Poor
IT team	36%	41%	18%	6%
Legal team	33%	36%	21%	11%
Executive management	30%	38%	22%	10%
Board of directors (or similar oversight body)	25%	34%	26%	16%
HR	23%	37%	24%	16%

0%   20%   40%   60%   80%   100%

How to Improve Relationships Between Security and IT Teams

Regardless of the status, which of the following actions could be most impactful for improving the working relationship between the <u>security and IT</u> teams at your organization? (Percent of respondents, N=275, three responses accepted)
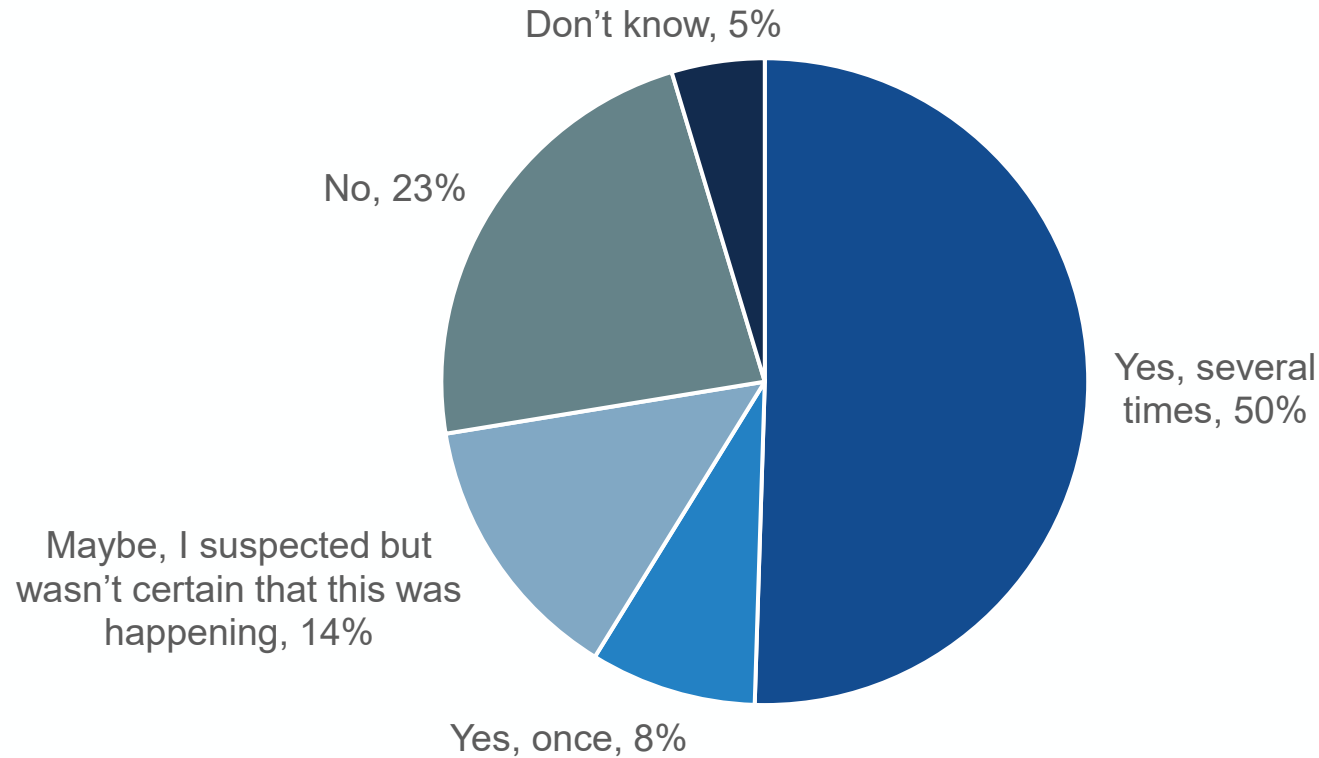
Action	Percent
Ensure that appropriate security staff is included in all IT projects from their start	55%
Increase cross-training between cybersecurity and IT staff	42%
Automate processes that require collaboration between IT and security teams	38%
Embed cybersecurity staff members into functional technology groups	29%
Standardize on common data sets and tools that can be used across security and IT	19%
Adopt a secure development lifecycle	18%
Alter employee compensation so that security and IT teams are rewarded to achieve common goals and objectives	16%
Adopt a DevSecOps model	14%
Other	7%
Don't know	7%

How to Improve Relationships Between Security and Business Managers

Regardless of the status, which of the following actions could be most impactful for improving the working relationship between the <u>security and business management</u> (i.e., line of business managers, corporate executives, etc.) teams at your organization?

|	
Improve our ability to identify and quantify cyber-risks as they apply to the business	44%
Increase cybersecurity training for executives and corporate boards	37%
Focus cybersecurity resources and investments on business-critical assets	35%
Establish one or more positions for business information security officers who would align cybersecurity with line-of-business processes and goals and build KPIs and metrics that align with the business mission	30%
Provide more business training for cybersecurity staff	29%
Increase CISO participation with executive management and corporate boards, including business planning and strategy	28%
Establish a formal enterprise security program that can be shared and adjusted based upon business input	26%
Other	3%
Don't know	5%

At any time in your career, have you experienced a situation in which the organization you worked for was knowingly ignoring security best practices and/or regulatory compliance requirements? (Percent of respondents, N=301)

Don't know, 5%

No, 23%

Maybe, I suspected but wasn't certain that this was happening, 14%

Yes, once, 8%

Yes, several times, 50%

Career History With Organizations Apathetic to Cybersecurity

If you were put in a situation in which the organization you worked for knowingly ignored security best practices and/or regulatory compliance requirements, despite warnings from the security team, would you be willing to act as a whistleblower? (Percent of respondents, N=301)

Don't know, 10%

No, 9%

Yes, 48%

Maybe, 33%
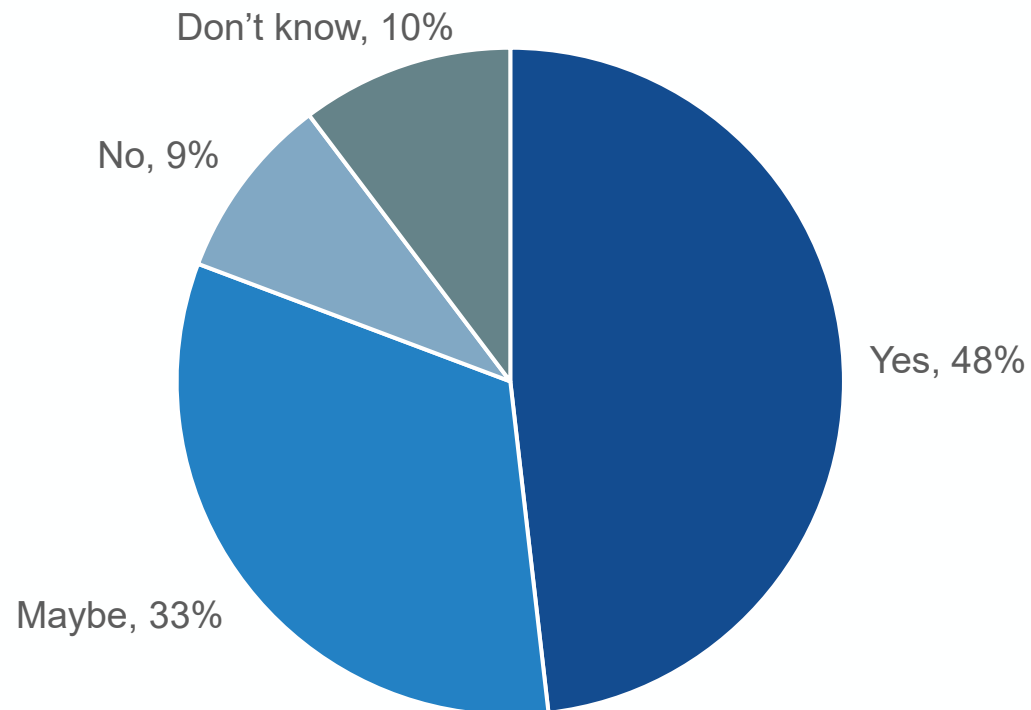
Willingness to Be a Cybersecurity Whistleblower

Actions to Improve Cybersecurity Culture Include Making It a Business Priority

What, if anything, could your organization do to improve its cybersecurity culture? (Percent of respondents, N=301, three responses accepted)

Action	Percent
Include cybersecurity early on in all future business plans	41%
Make managers more accountable for cybersecurity performance	36%
Provide more/better security awareness training to non-technical employees	30%
Emphasize security best practices rather than regulatory compliance	29%
Measure and compensate the entire organization based on cybersecurity metrics	21%
Increase cybersecurity training for IT and software development personnel	21%
Add someone with cybersecurity knowledge to the board of directors	20%
Embed cybersecurity personnel within lines of business	20%
Create security metrics for IT and software development personnel	18%
Increase the level of CISO involvement with executives and the board of directors	17%
Other	3%
Don't know	5%

Improving Cybersecurity Programs Through Training and Hiring

Which of the following actions do you believe your organization could take to improve its cybersecurity program? (Percent of respondents, N=301, multiple responses accepted)
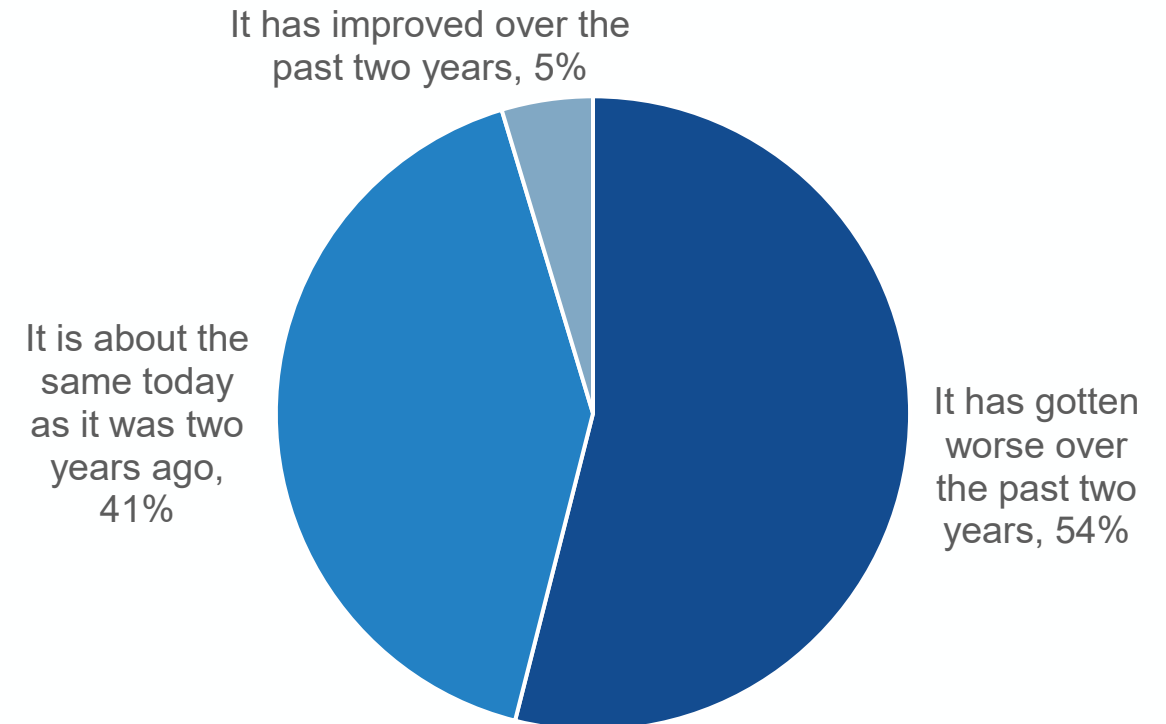
Action	Percent
Increase training for cybersecurity and IT professionals	50%
Strive to create a better cybersecurity culture throughout the organization	45%
Hire more staff	44%
Increase the cybersecurity budget	39%
Improve our basic security hygiene and posture management	35%
Increase security awareness training for non-technical employees	33%
Improve our ability to prevent, detect, and respond to threats in a timely manner	33%
Conduct more frequent testing to validate our security controls and identify areas of weakness	29%
Get executives and the board of directors more involved in cybersecurity oversight and decision making	29%
Change the reporting structure so the CISO reports directly to the CEO	18%
Outsource more security responsibilities to third-party security service providers	7%
Other	10%
Don't know	4%

Cybersecurity Skills Shortage

Enterprise Strategy Group™
by TechTarget

Impact and Status of the Global Cybersecurity Skills Shortage

There has been a lot written about the global cybersecurity skills shortage. Has this trend impacted the organization for which you currently work? (Percent of respondents, N=301)

Don't know, 6%

Yes, significantly, 27%

No, 23%

Yes, somewhat, 44%
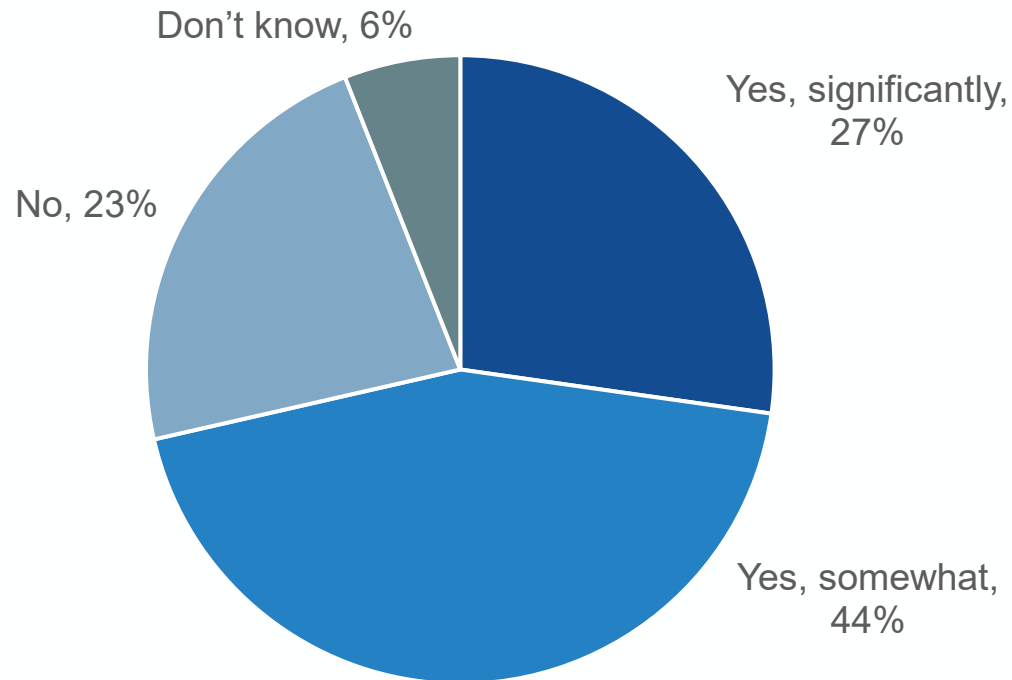
How do you think the cybersecurity skills shortage and its impact on your organization has changed over the last two years? (Percent of respondents, N=215)

It has improved over the past two years, 5%

It is about the same today as it was two years ago, 41%

It has gotten worse over the past two years, 54%

Factors Contributing to the Skills Shortage Impact

Which of the following are the biggest factors contributing to the cybersecurity skills shortage's impact on your organization? (Percent of respondents, N=215, three responses accepted)

Factor	Percent
My organization doesn't offer competitive compensation, making it difficult to recruit/hire cybersecurity professionals	47%
The HR department at my organization really doesn't understand the skills needed for cybersecurity, so it probably excludes strong candidates and our job postings tend to be unrealistic	34%
My organization doesn't do enough outreach to the cybersecurity community	33%
My organization doesn't have a reputation as a cybersecurity leader, making it difficult to recruit/hire new cybersecurity professionals	28%
My organization is in an industry that may not be attractive for cybersecurity professionals	28%
My organization tends to recruit IT and cybersecurity professionals rather than qualified applicants with more diverse backgrounds	24%
My organization is not located in a major metropolitan area where we would have access to more cybersecurity professionals	6%

Impact of the Cybersecurity Skills Shortage

What type of impact do you believe the global cybersecurity skills shortage has had on your organization? (Percent of respondents, N=215, multiple responses accepted)

Impact	Percent
Increasing workload on existing staff	61%
New security jobs remain open for weeks or months	49%
High "burnout" and/or attrition rate among the cybersecurity staff	43%
Inability to fully learn or utilize some of our security technologies to their full potential	39%
My organization has hired and trained junior employees rather than experienced candidates	30%
Cybersecurity staff has limited time to work with business units	28%
Cybersecurity staff time is spent disproportionally on high-priority issues and incident response	28%
Increase in the use of professional and/or managed services	27%
My organization has delegated some security tasks to IT that it would normally do itself	19%
An increase in human error associated with cybersecurity tasks	19%
Inability to investigate and/or prioritize security alerts in a timely manner	18%

Most Significant Areas of Cybersecurity Skills Shortage

In which of the following areas, if any, would you say that your organization has the most significant shortage of cybersecurity skills? (Percent of respondents, N=215, three responses accepted)

Area	Percent
Application security	38%
Cloud computing security	37%
Security analysis and investigations	27%
Security engineering	26%
Senior-level cybersecurity positions	24%
Risk and/or compliance administration	20%
Penetration testing/red teaming	14%
Network security	12%
Mobile computing security	11%
Security auditors	10%
Endpoint security	9%
Database security	6%
Other	5%
Don't know	5%
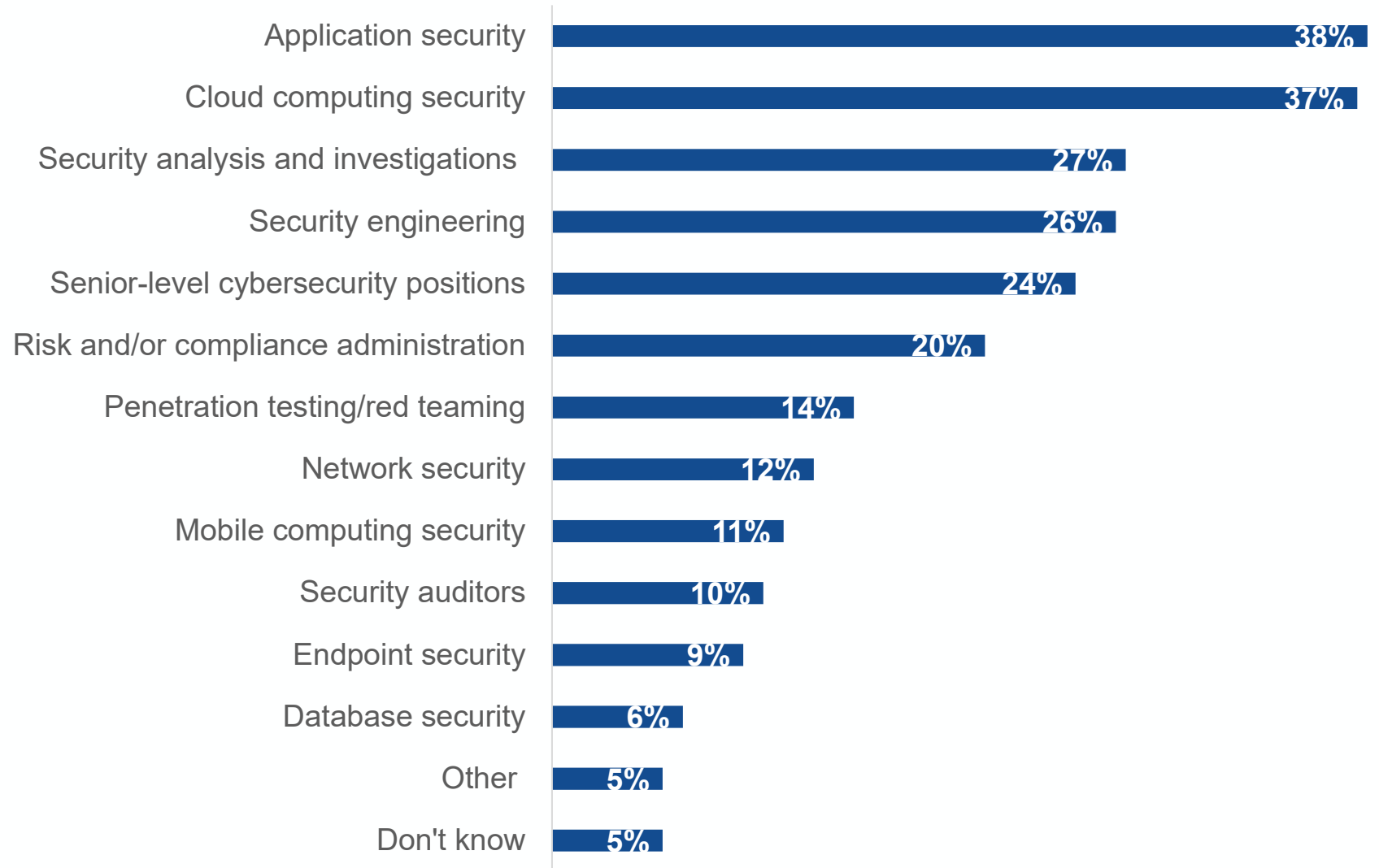
Majority of Security Professionals Believe Their Organizations Could Do More to Mitigate Cybersecurity Skills Shortage

Do you believe your organization is taking the necessary actions to address the impact of the cybersecurity skills shortage? (Percent of respondents, N=215)

Yes	No, my organization could be doing much more	No, my organization could be doing slightly more	Don't know
27%	36%	24%	13%
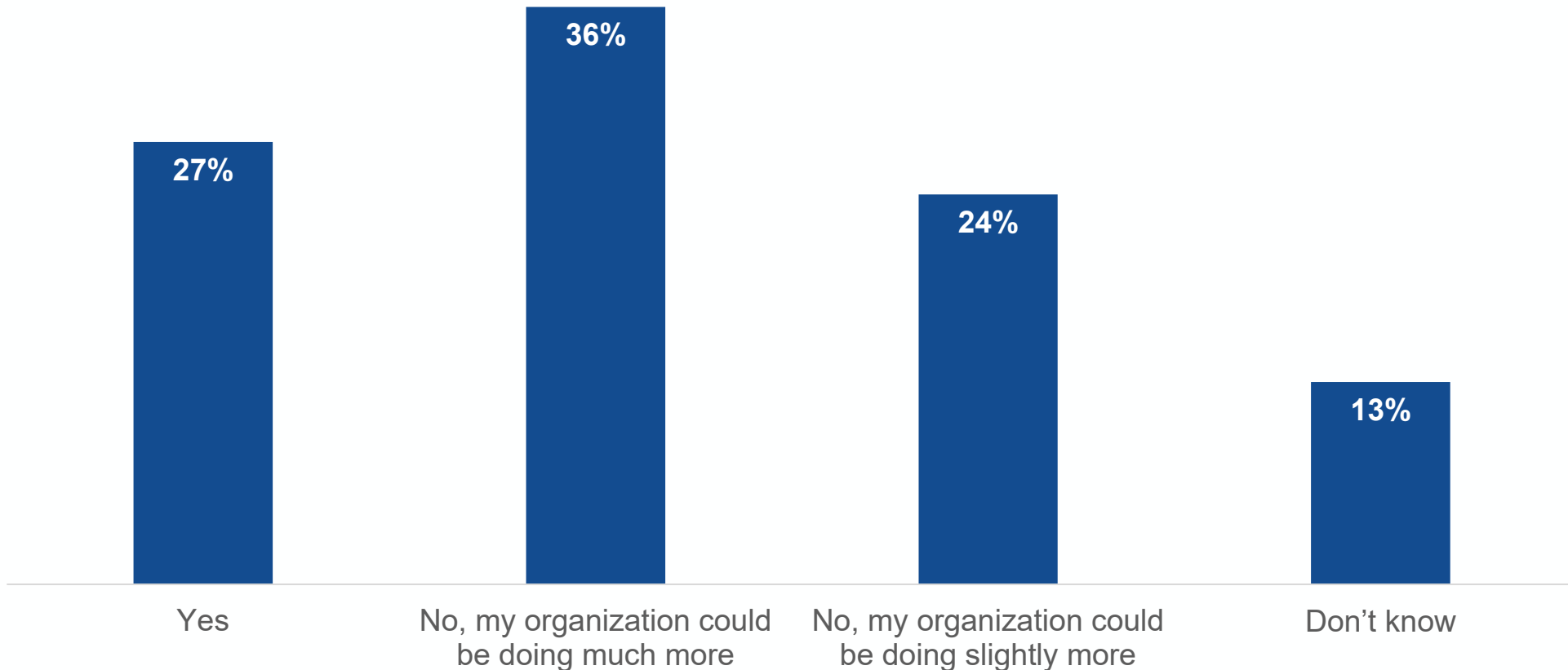
Addressing the Impact of the Cybersecurity Skills Shortage

What actions do you believe your organization could take to address the impact of the cybersecurity skills shortage? (Percent of respondents, N=129, multiple responses accepted)

Action	Percent
Increase compensation levels to make them competitive with other organizations in our industry/geography	59%
Provide incentives like paying for certifications and participation in industry events as part of compensation packages	52%
Better educate HR and recruiters on our cybersecurity needs so they can better target recruitment	41%
Increase its commitment to cybersecurity training so we can bring in candidates and train them on what we need them to do	40%
Create/improve a cybersecurity internship program and increase its recruiting efforts with colleges/universities	40%
Modify job requirements so they are more realistic with the typical levels of experience cybersecurity professionals have	39%
Work with cybersecurity professional organizations like ISSA on job descriptions, recruiting, etc.	26%
Look beyond IT and security professionals to find qualified candidates in other disciplines	21%
Offload some cybersecurity tasks/processes to managed security service providers (MSSPs)	18%
Delegate some cybersecurity tasks/processes to IT	12%
Other	8%

Nearly One-third of Security Pros Believe the Cybersecurity Skills Shortage Is <u>Understated</u>

Regardless of what is happening at your organization, in your opinion, which of the following statements about the industry discussions regarding the cybersecurity skills shortage is most accurate? (Percent of respondents, N=301)

Greatly overstated (i.e., skills shortage is not a problem at all)	3%
Somewhat overstated (i.e., skills shortage is a minor problem)	21%
About right	44%
Somewhat understated (i.e., skills shortage is a substantial problem)	22%
Greatly understated (i.e., skills shortage is a significant problem)	10%
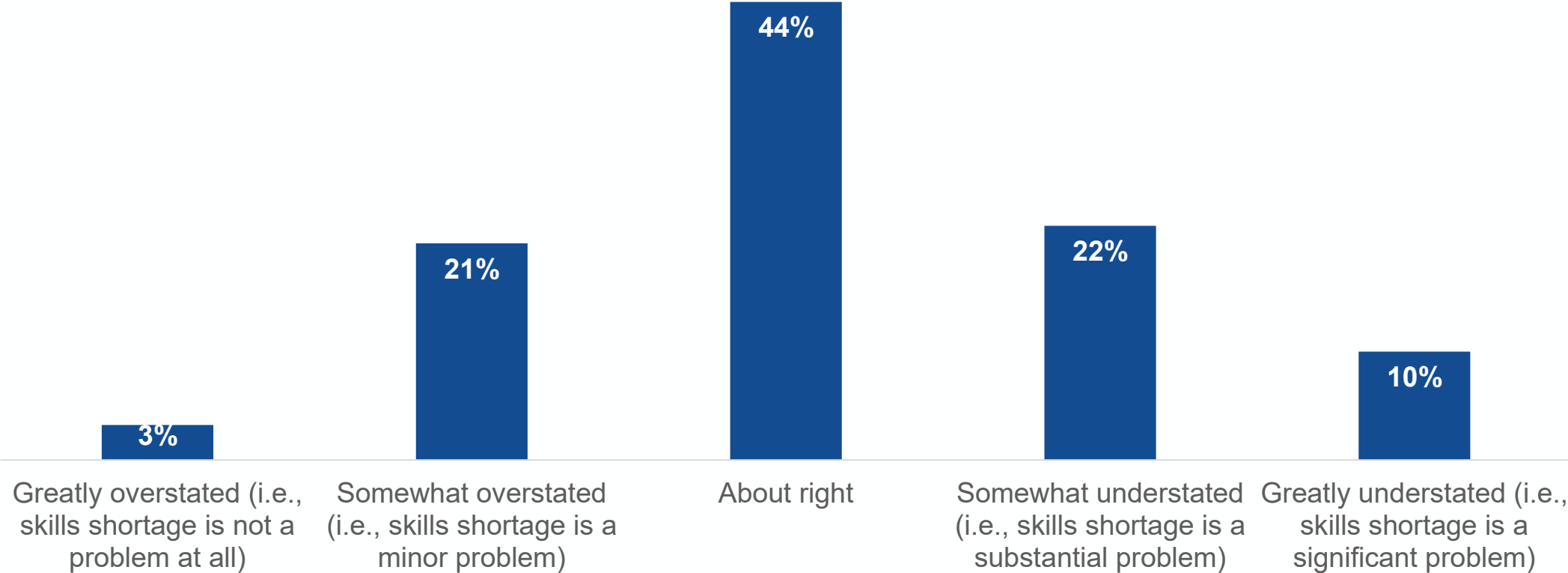
Challenges Recruiting Mid-career Cybersecurity Professionals

How difficult is it for your organization to recruit and hire cybersecurity professionals? (Percent of respondents, N=301)

Extremely difficult	Difficult	Somewhat difficult	Not at all difficult
19%	39%	29%	12%
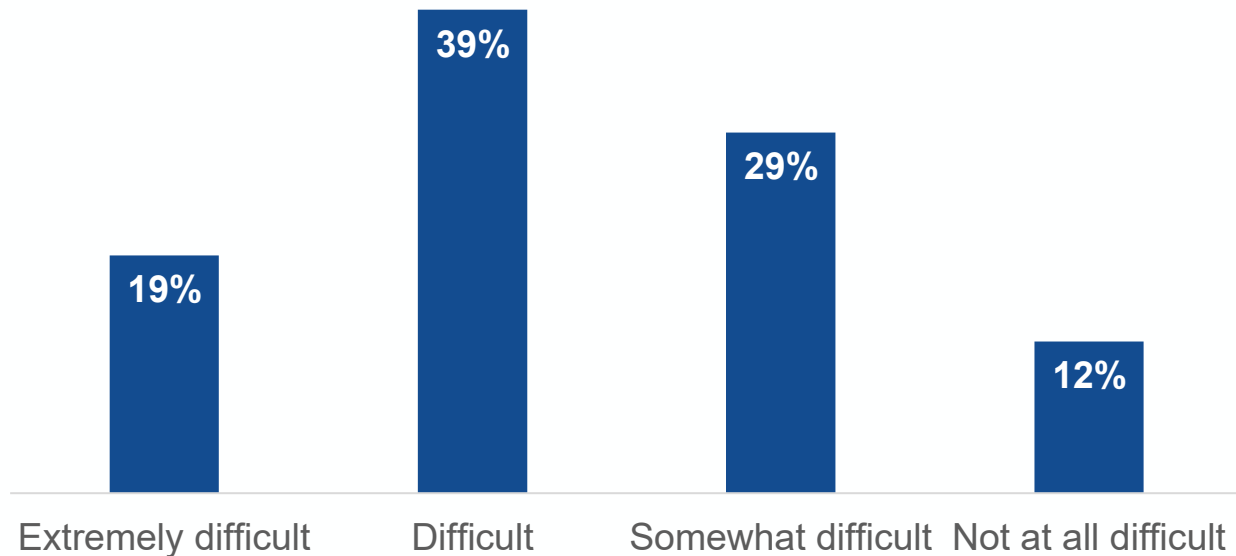
Based on amount of experience, which group of cybersecurity professionals has been most challenging for your organization in terms of recruiting and hiring? (Percent of respondents, N=301)

Entry (1-3 years on-the-job experience)	Mid-career (4-7 years on-the-job experience)	Senior (7+ years on-the-job experience)	Leader (7+ years on-the-job experience and responsible for strategy)
12%	42%	33%	13%

Cybersecurity Leadership

Enterprise Strategy Group™
by TechTarget
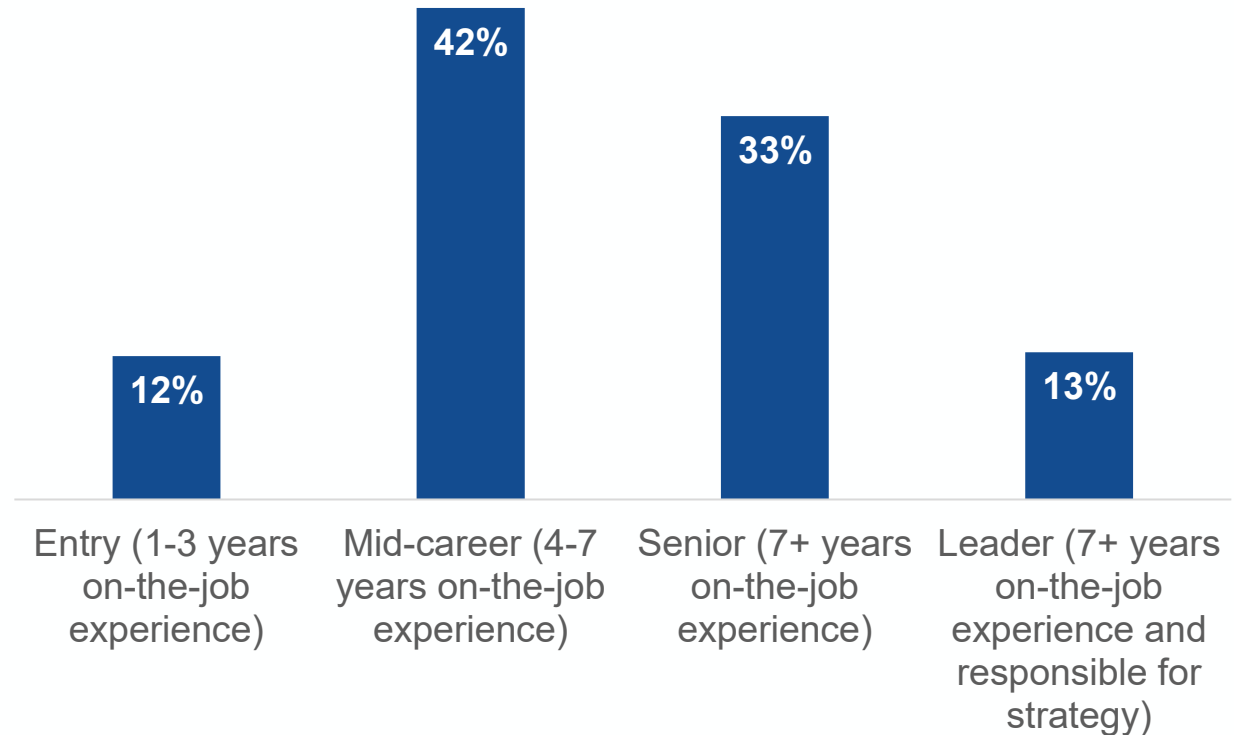
Does your organization have a chief information security officer (CISO) (or similar position) in place today? (Percent of respondents, N=301)
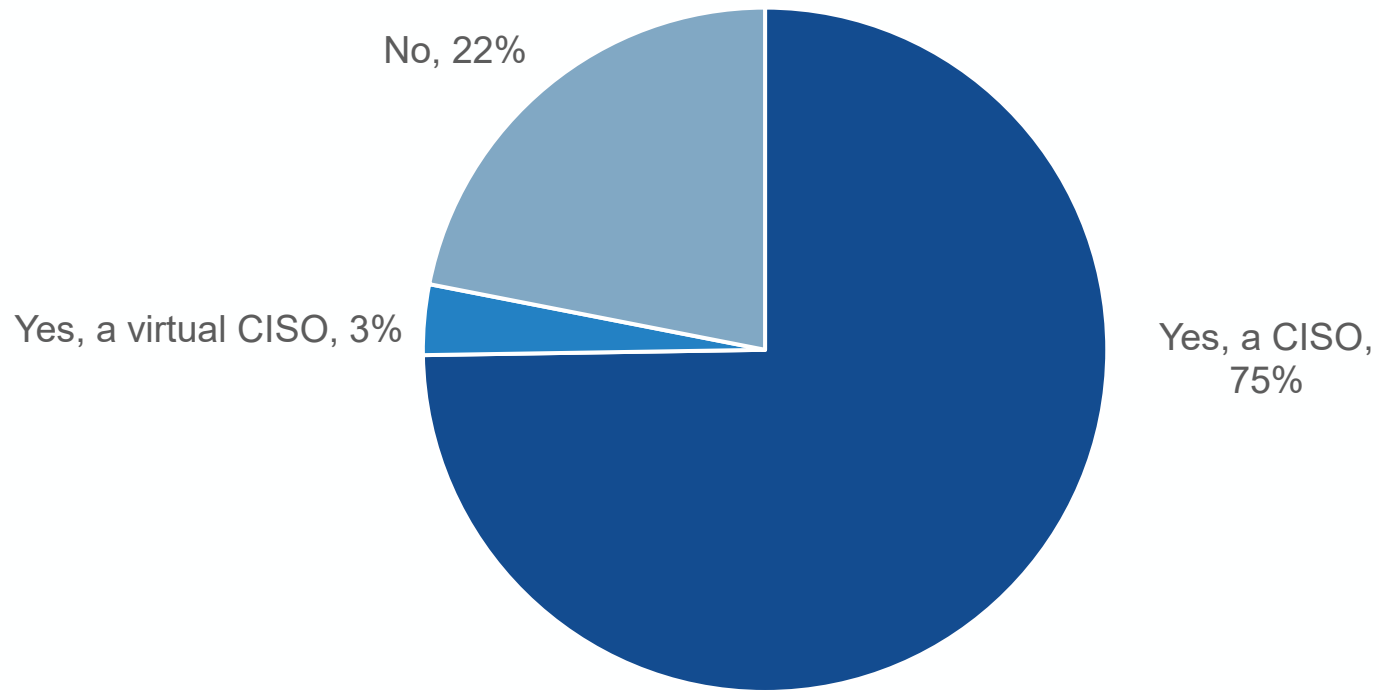
Vast Majority of Organizations Report Having a CISO

No, 22%

Yes, a virtual CISO, 3%

Yes, a CISO, 75%

CISOs Commonly Report to CIOs and Interact with BoD

Which of the following best represents to whom the CISO reports? (Percent of respondents, N=235)

Don't know, 6%

Other, 12%

COO, 9%

CIO or other senior IT person, 49%

CEO, 24%
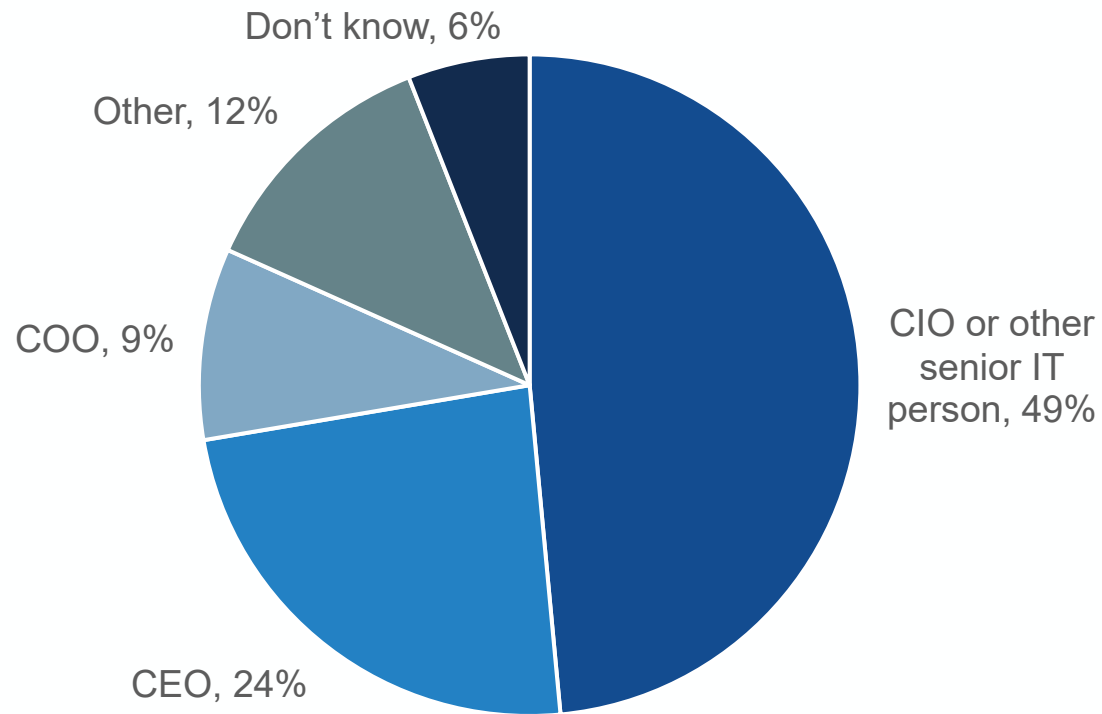
Does your organization's CISO actively interact with executive management and the board of directors (or similar oversight group)? (Percent of respondents, N=235)

Don't know, 18%

No, 10%

Yes, 72%
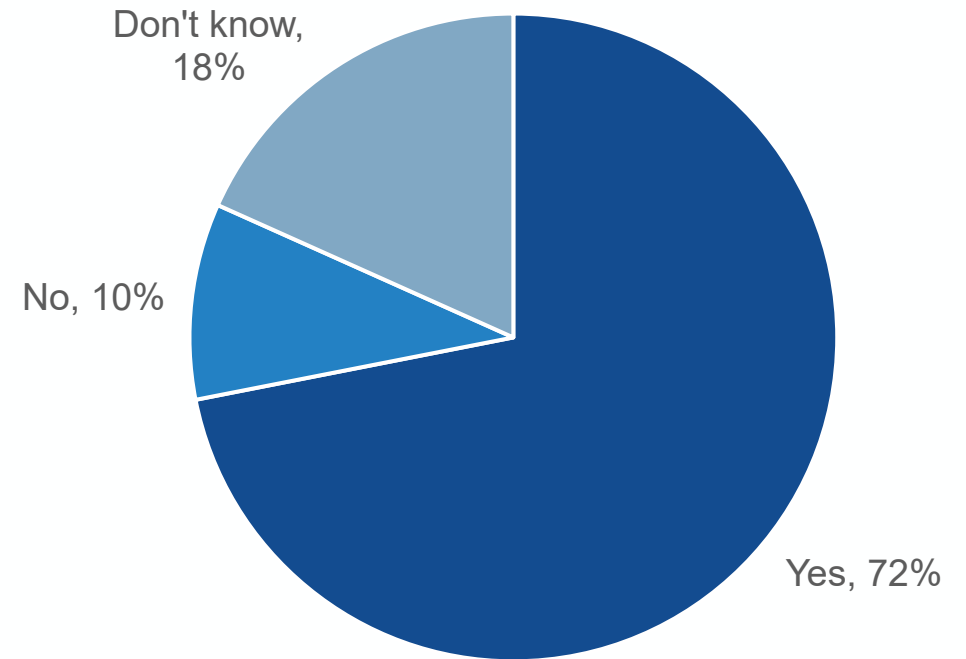
Most Believe Their CISOs Are Effective But Could Do a Better Job Interfacing With Executives and BoD

In your opinion, how effective has your CISO been? (Percent of respondents, N=235)
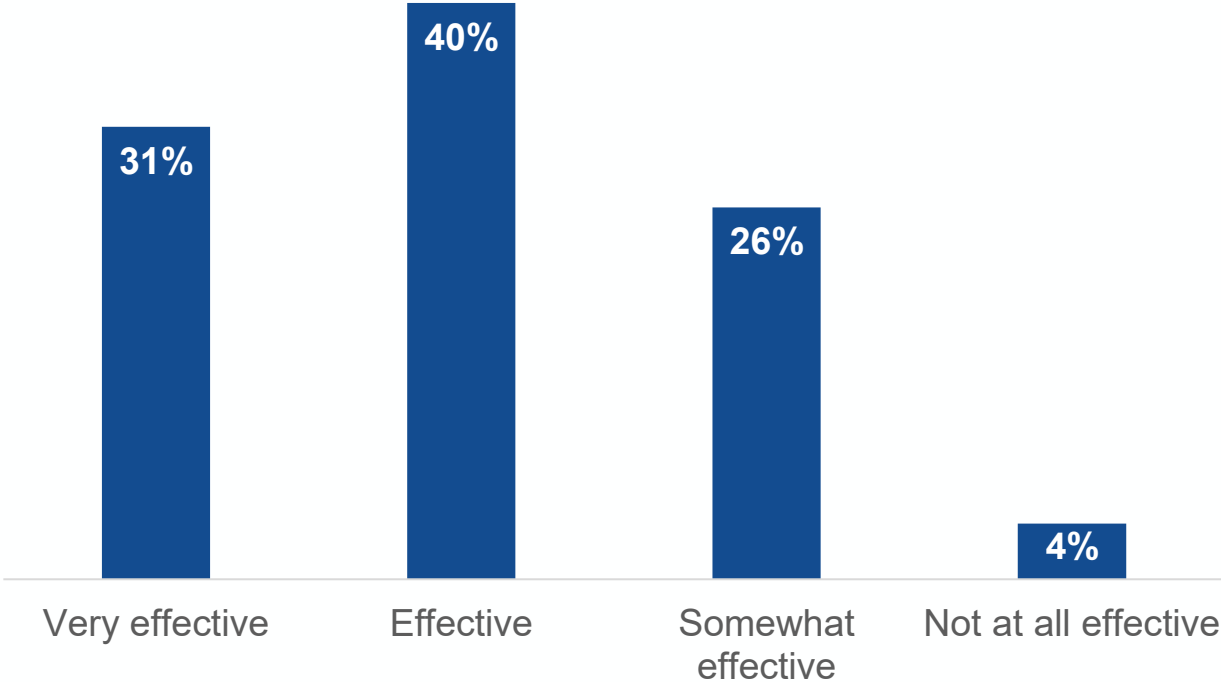
Do you think your organization's CISO's level of participation with executive management and the board of directors is adequate? (Percent of respondents, N=235)

- Very effective: 31%
- Effective: 40%
- Somewhat effective: 26%
- Not at all effective: 4%

- Yes, 49%
- No, 27%
- Don't know, 24%
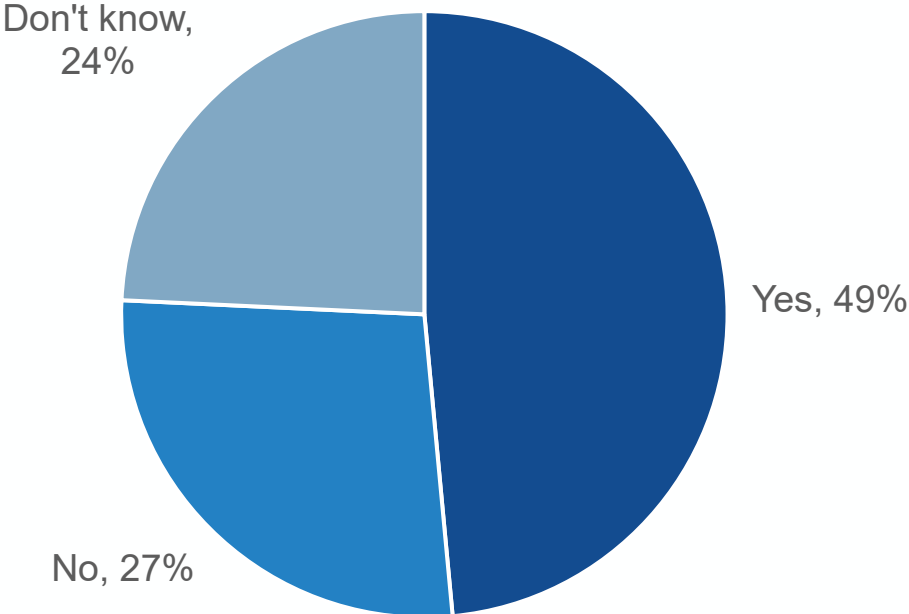
In your opinion, which of the following is the most important quality of a successful CISO? (Percent of respondents, N=301)

Don't know/no opinion, 1%

Other, 2%

Operational skills, 5%

Technical skills, 5%

Management skills, 7%

Business skills, 10%

Communications skills, 33%

Leadership skills, 38%
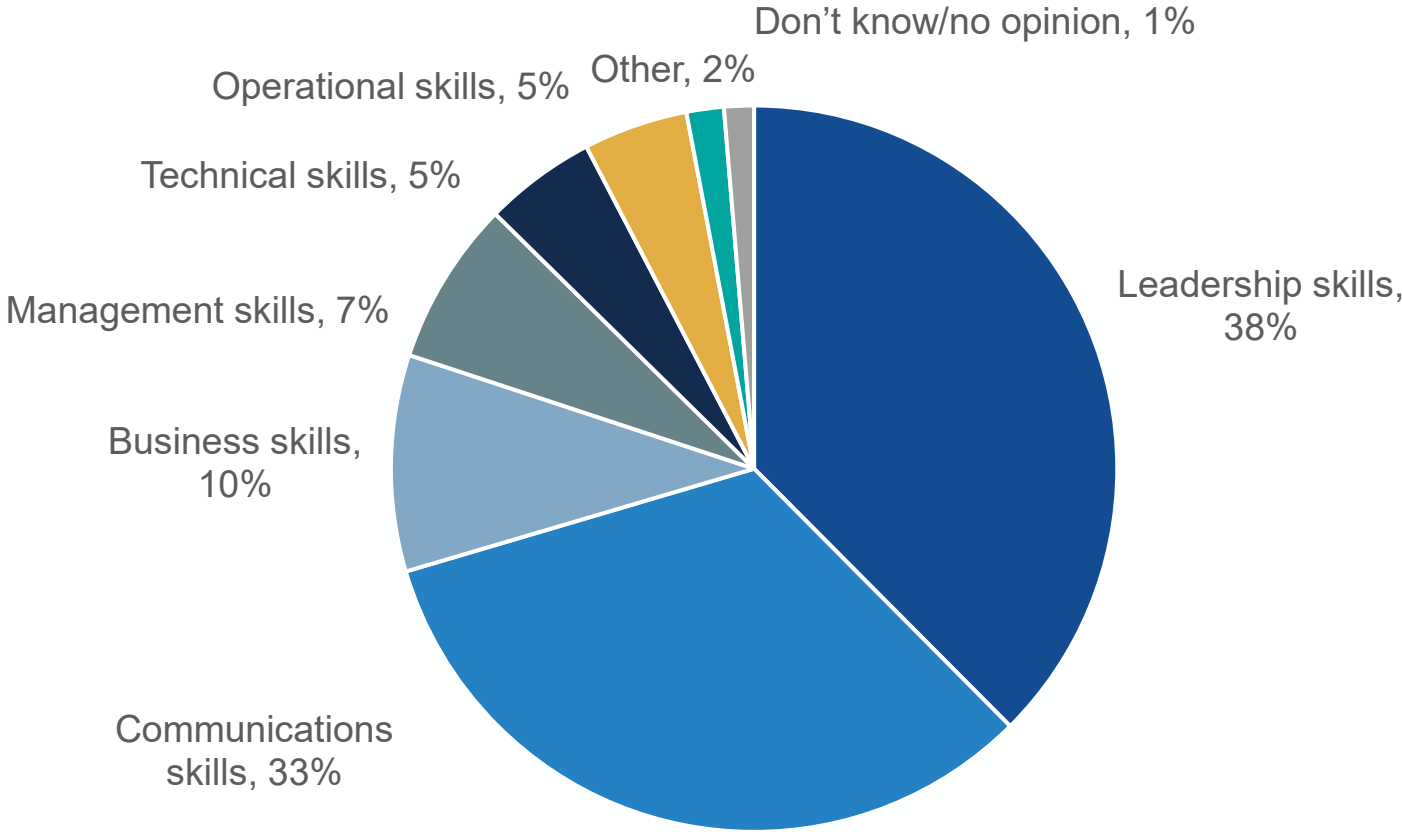
Leadership and Communications Skills Are Important Qualities for Successful CISOs

Reasons CISOs Change Jobs

In your opinion, which of the following factors are likeliest to cause CISOs to leave one organization for another? (Percent of respondents, N=301, three responses accepted)

Factor	Percent
CISOs are offered a higher compensation package at another organization	35%
Cybersecurity budgets are not commensurate with the organization's size and industry	33%
CISOs are prone to "burnout" and change jobs as a result	28%
Organization does not have a corporate culture that emphasizes cybersecurity	26%
CISO is not an active participant with executive manager and/or board of directors	26%
CISO discovers that executive management does not understand cybersecurity at a level commensurate with the organization's size and…	26%
Organization treats cybersecurity as a regulatory compliance issue	23%
Cybersecurity staffing levels are not commensurate with the organization's size and industry	22%
CISO discovers that the organization's cybersecurity policies, procedures, and technologies are greatly inadequate	14%
CISO is not comfortable with the reporting structure at their organization	13%
Other	3%
Don't know	6%

Respondent Demographics/ Firmographics

Enterprise Strategy Group
by TechTarget

Respondents by Region

In what region are you located? (Percent of respondents, N=301)

Region	Percent
North America	86%
Europe	6%
Asia	4%
Africa	2%
Central/South America	2%
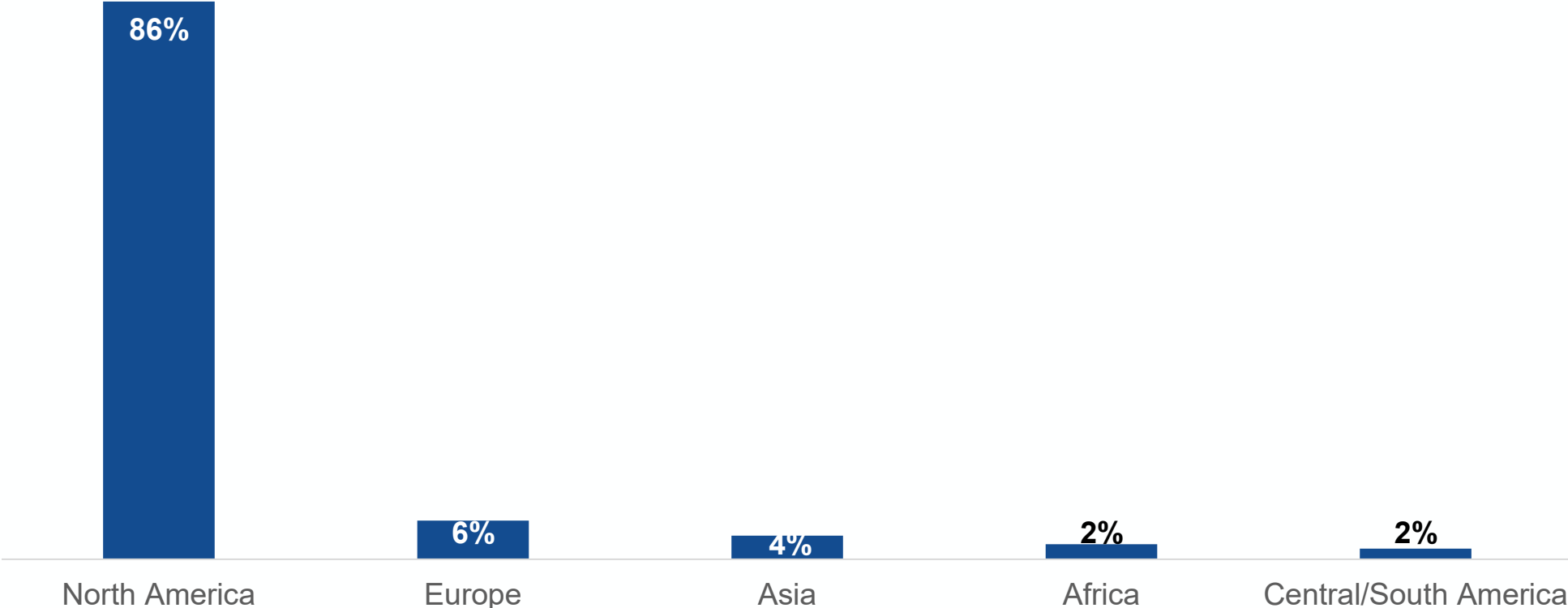
Respondents by Current Position

Which of the following best describes your current position within your organization? (Percent of respondents, N=301)

Position	Percent
CISO, CSO, or similar senior cybersecurity position	17%
Director-level position in an information security department	16%
Security administrator	14%
IT staff	14%
IT management	12%
VP-level position in an information security department	5%
Other	22%
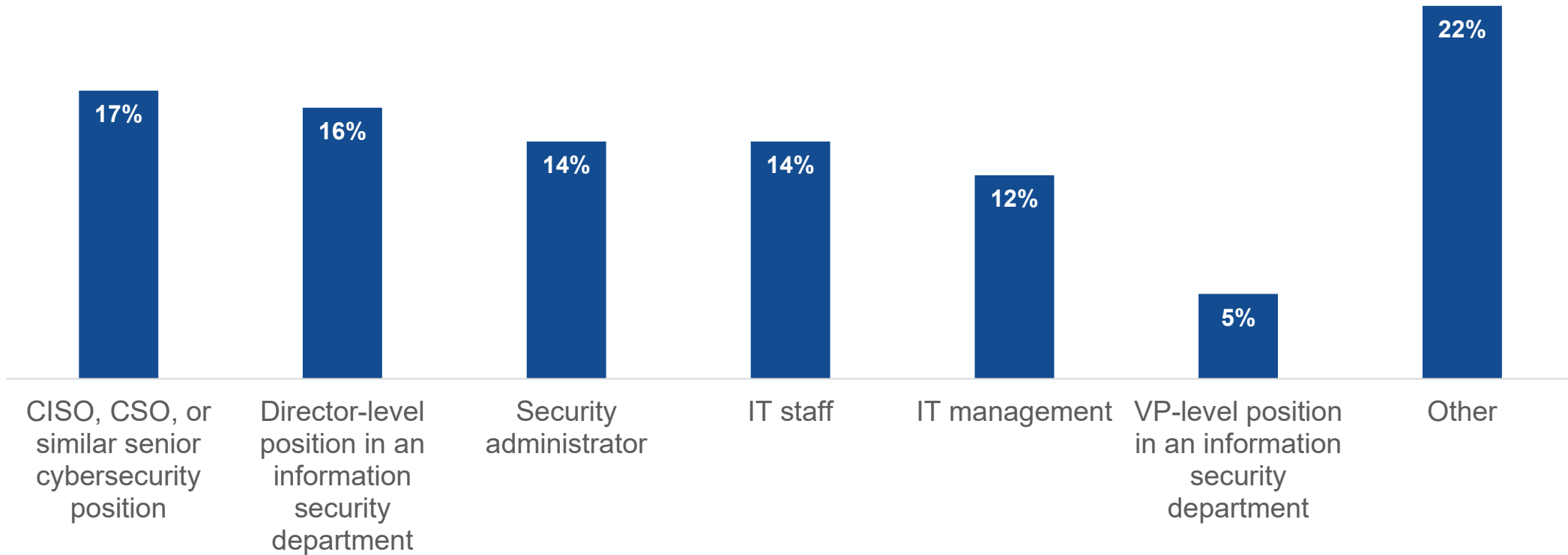
Which of the following best describes your overall job responsibilities? (Percent of respondents, N=301)

I split my time between cybersecurity and other functions (e.g., IT, DevOps, etc.), 36%

I am dedicated to cybersecurity (i.e., cybersecurity planning, operations, threat intelligence analysis, incident response, vulnerability management, etc.), 64%
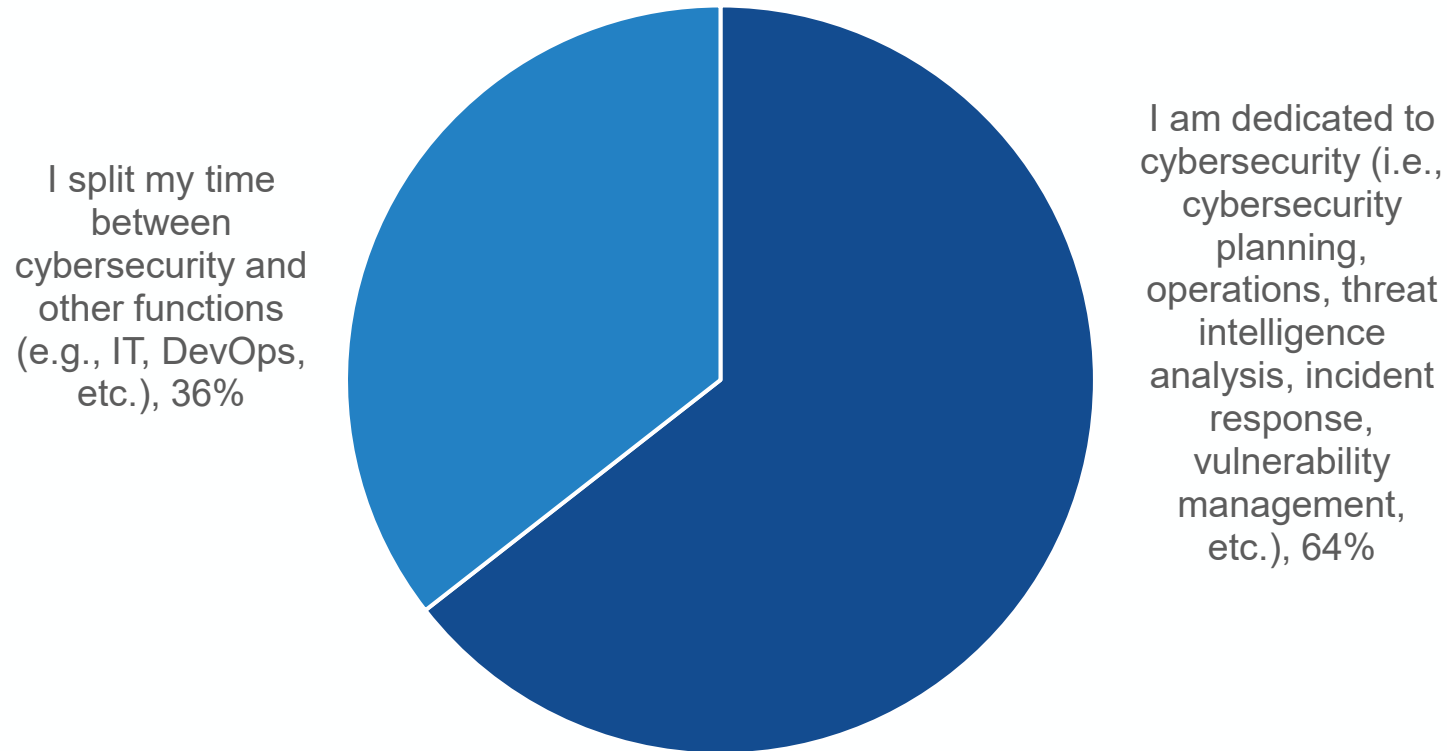
Respondents by Job Responsibilities

Respondents by Areas of Cybersecurity Responsibility

Which of the following **best** (i.e., most closely) describes your primary cybersecurity responsibilities within your organization? (Percent of respondents, N=301, three responses accepted)

Risk and vulnerability	44%
Governance/compliance	41%
System security	21%
Security analysis and planning	20%
Incident response	19%
Information security analyst/investigator	16%
Cloud security	16%
Network security	15%
Information security engineering	13%
Information security auditing	12%
Information assurance	12%
Identity and access management	11%
Application security	11%
Penetration testing	2%

Respondents by Number of Employees

How many total employees does your organization have worldwide? (Percent of respondents, N=301)

Chart showing percent of respondents by number of employees:
- Fewer than 50: 13%
- 50 to 99: 9%
- 100 to 499: 7%
- 500 to 999: 9%
- 1,000 to 2,499: 10%
- 2,500 to 4,999: 10%
- 5,000 to 9,999: 7%
- 10,000 to 19,999: 12%
- 20,000 or more: 22%
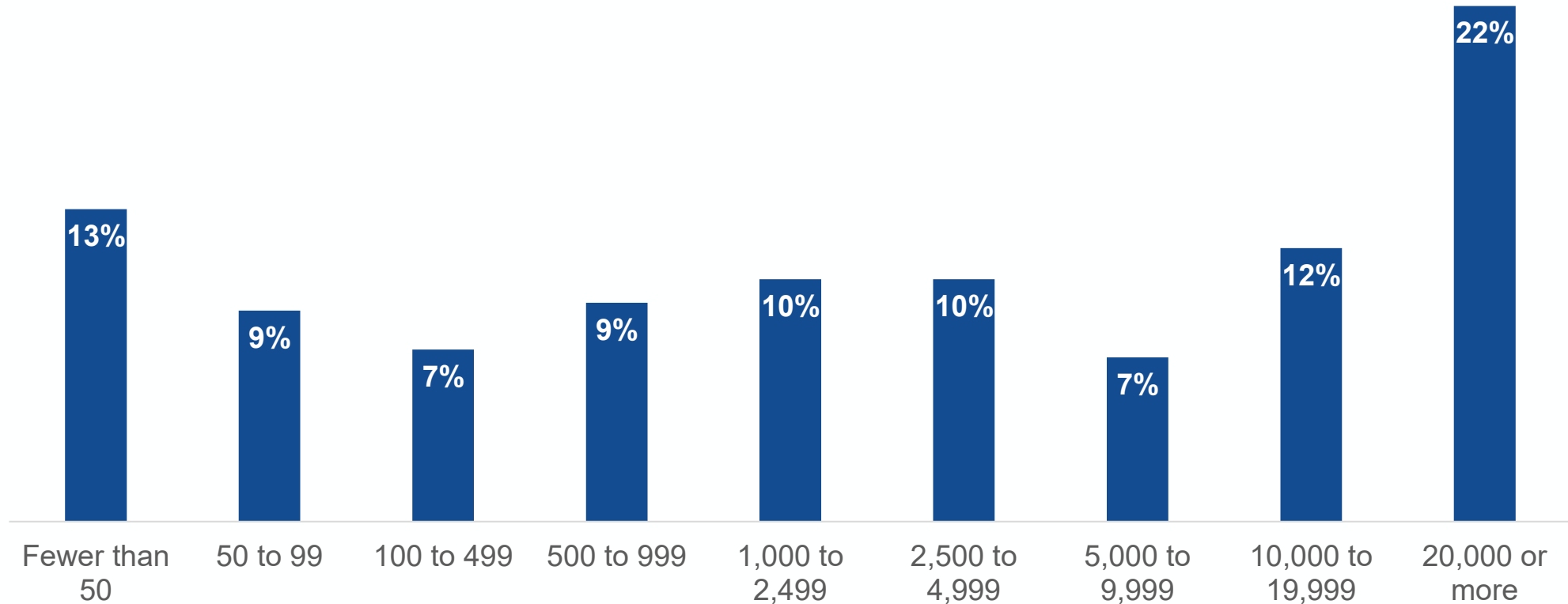
Respondents by Industry

What is your organization's primary industry? (Percent of respondents, N=301)

Industry	Percent
Technology	21%
Government	16%
Financial	14%
Business services	12%
Healthcare	7%
Manufacturing	6%
Communications and media	5%
Retail/wholesale	2%
Other	16%
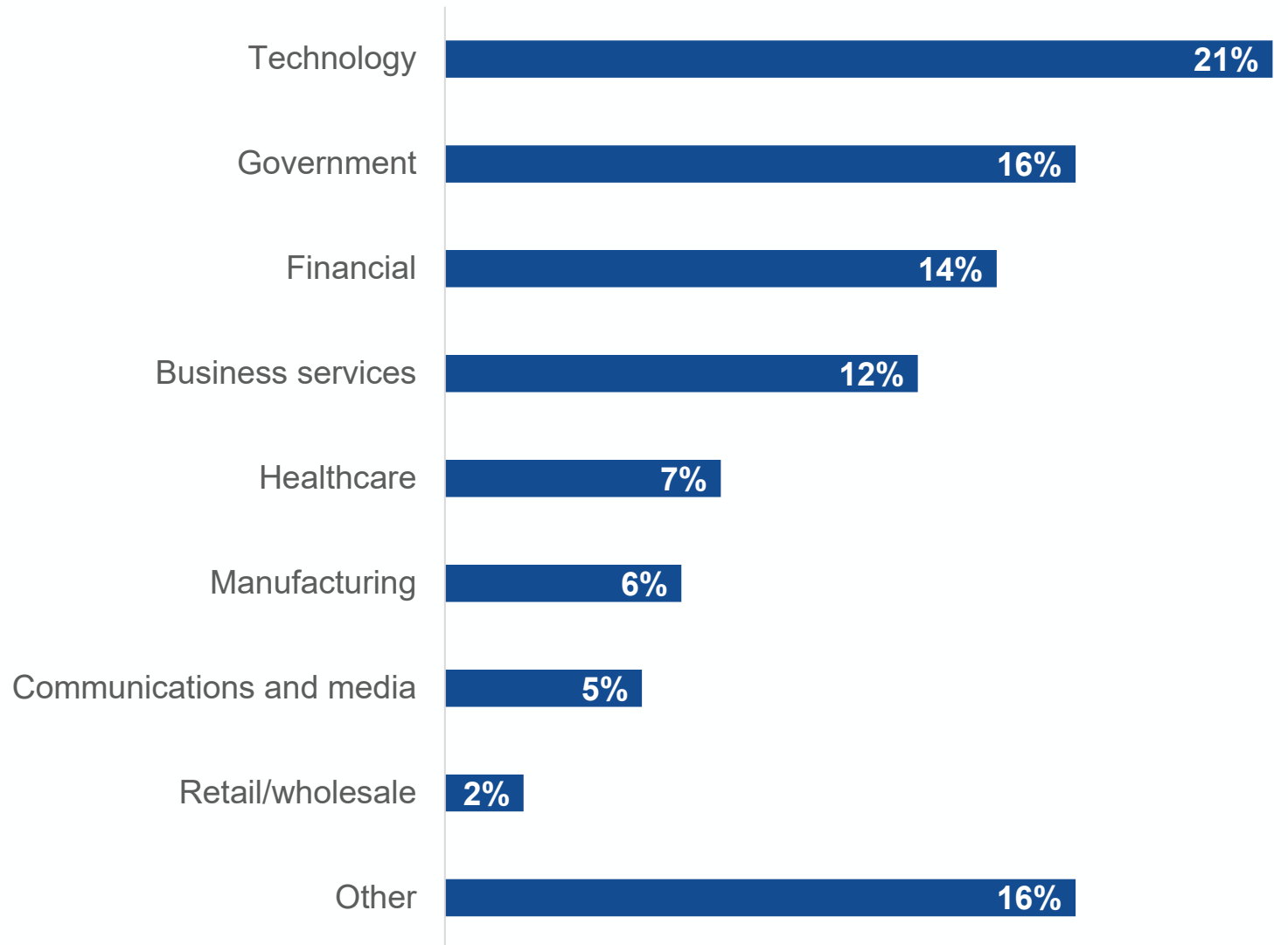
Respondents by Annual Revenue

What is your organization's total annual revenue ($US)? (Percent of respondents, N=301)

Category	Percent
Less than $100 million	29%
$100 million to $249.999 million	6%
$250 million to $499.999 million	7%
$500 million to $999.999 million	5%
$1 billion to $4.999 billion	11%
$5 billion to $9.999 billion	8%
$10 billion to $19.999 billion	6%
$20 billion or more	18%
Not applicable (e.g., public sector, non-profit)	12%

Enterprise Strategy Group™

by **TechTarget**
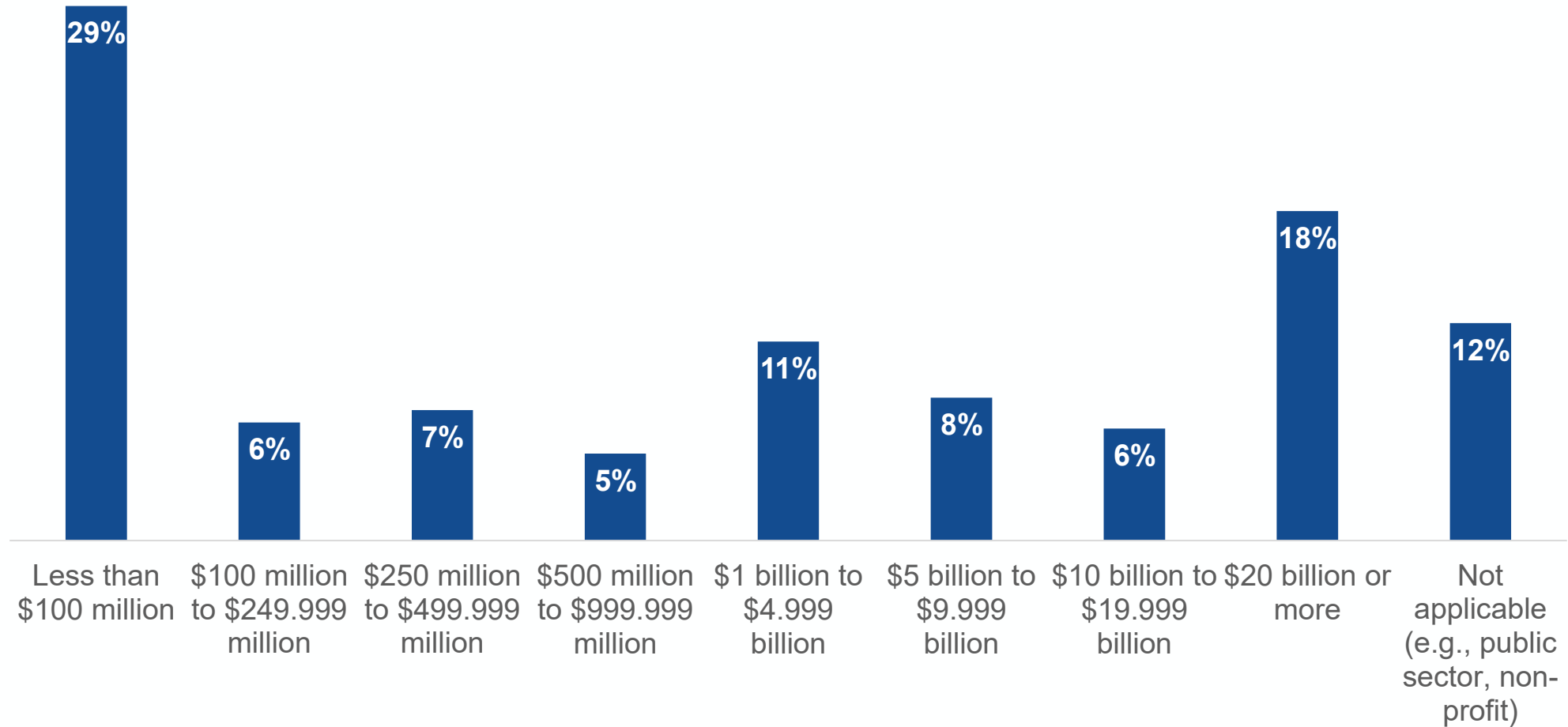
For questions about this data set, please email

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.