coretelligent

C-Suite Cybersecurity Report 2024

→ Mid-market Leadership and Reframing Cybersecurity for Business Resilience

In August 2024 we fielded a **cybersecurity pulse-check survey of mid-market C-suite executives.**

Aimed at benchmarking how this group approaches growing and protecting their business at the same time, our survey pooled participants from a cross-section of U.S. companies in industries that are highly targeted by cybercriminals.

Data from their responses covers five trend areas →

01

Structure & Resources

67%

say their IT teams report directly to the CEO or CFO

02

Culture

65%

consider cybersecurity a “strategic priority and business enabler”

03

Confidence & Skills

83%

express high confidence in their cyber defense, but 44% cite gaps in intellectual property protection skills

04

AI & Emerging Tech

57%

are already using AI in their cybersecurity

05

The Future

46%

are “very concerned” about cybersecurity hampering their ability to innovate

As the business impacts of cyber incidents become more urgent, these trend areas show that **the mindset around cybersecurity – including a growing awareness of the importance of cyber resilience – is starting to evolve.** And according to our data, today’s mid-market C-suite executives are perfectly positioned to lead the charge.

01 Structure & Resources

→ *When it comes to cybersecurity, who's doing what and with what types of resources?*

Non-technical executives control the cybersecurity purse strings.

Survey participants share that even with a range of different technical leadership positions on staff at small- to mid market firms, more often than not, IT teams report directly to non-technical C-suite leaders, primarily CEOs and CFOs.

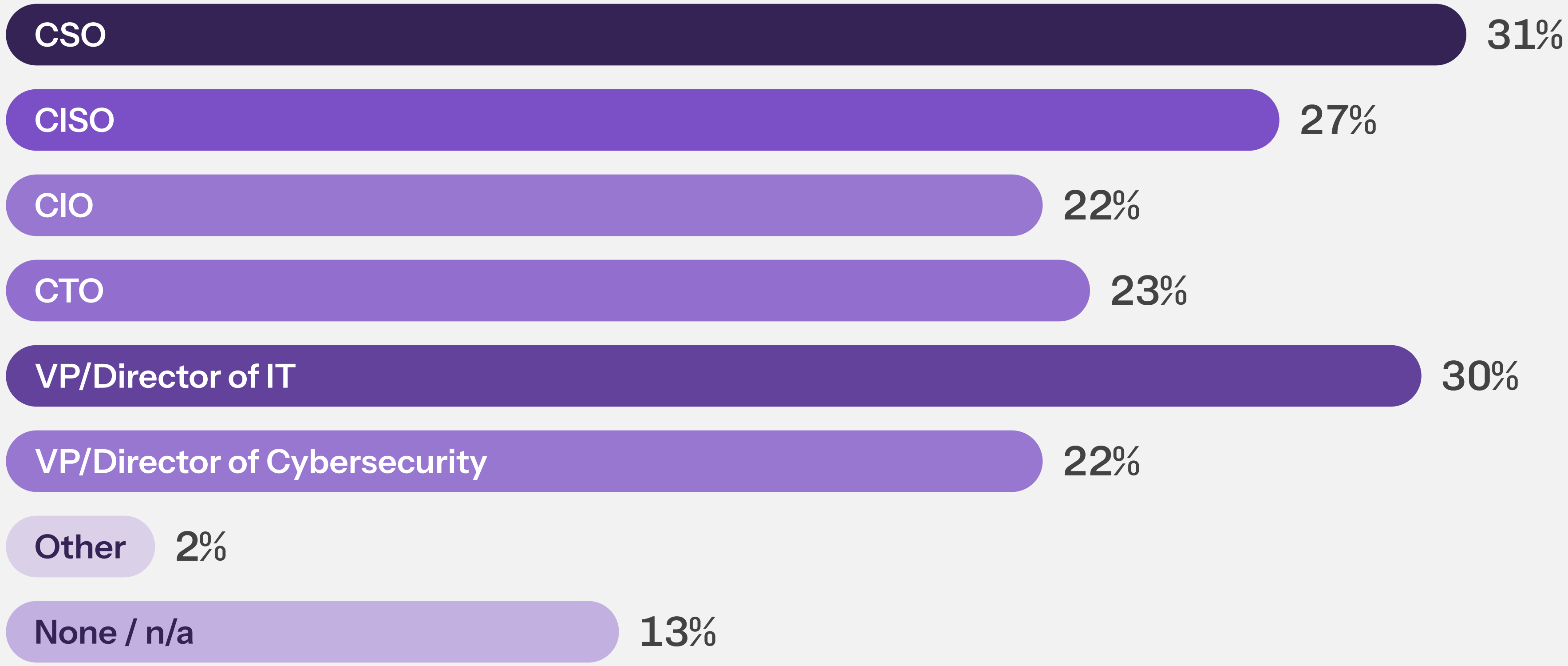
→ Q: Within your organization, who does your IT team report to?

84%

say their IT teams report directly to the C-suite.

67% report to the CEO (52%) or CFO (15%), and 17% say their IT teams report to a different C-suite leader.

→ Q: Which of the following IT leadership positions does your organization have? (check all that apply)



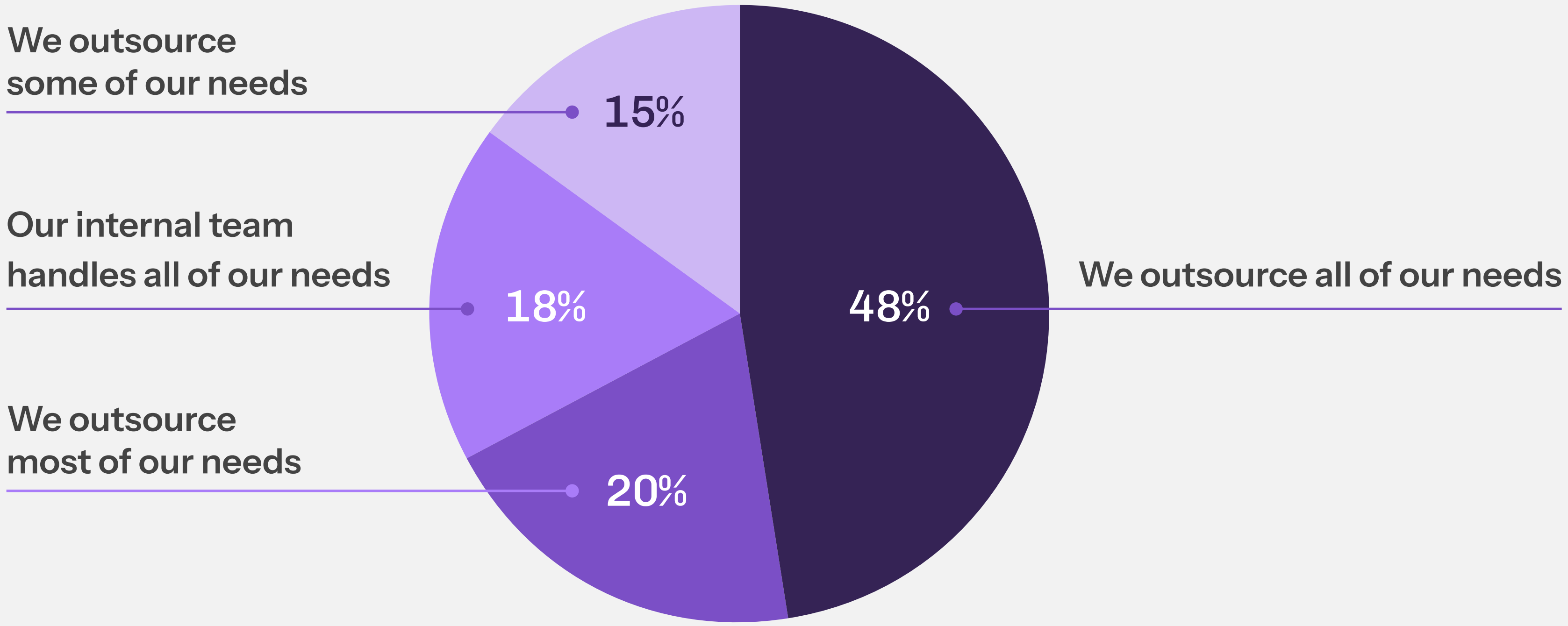
Looking at cybersecurity as a subset of IT, data shows the number of cybersecurity professionals that companies employ internally varies (the most popular answer being 2–4 employees), with nearly half of participants saying they outsource all of their cybersecurity and compliance staffing needs.

→ Q: How many dedicated internal cybersecurity professionals does your organization employ?

41% **say their organization employs 2–4 dedicated, internal cybersecurity professionals.**

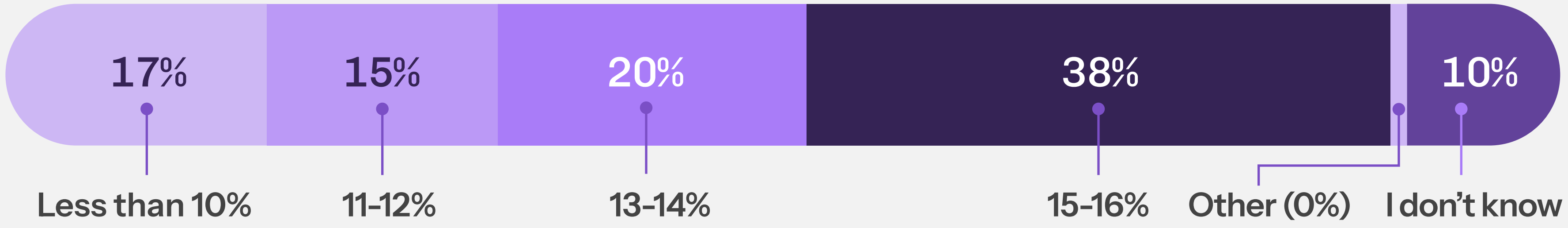
Meanwhile, 18% say their companies don't employ any cybersecurity professionals at all.

→ Q: To what extent does your organization rely on third-party vendors for cybersecurity and related compliance services?

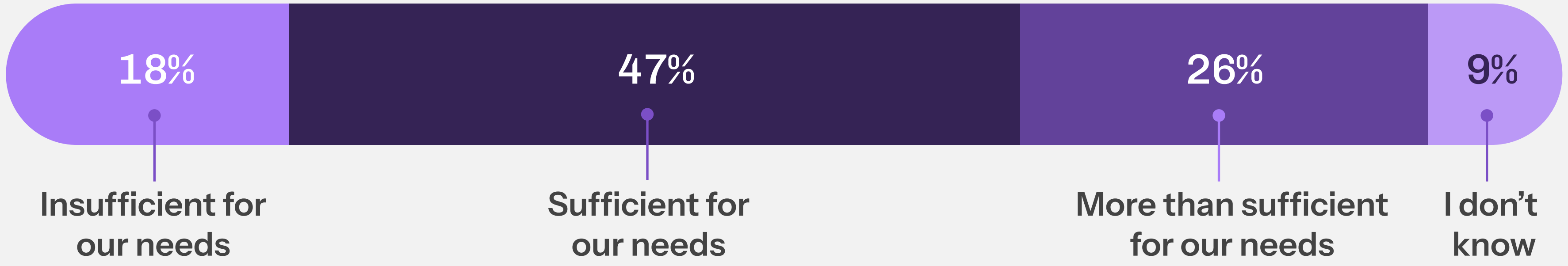


Respondents share that the amount of IT budget typically allocated to cybersecurity is 15–16%. Forty-seven percent say the amount being spent is sufficient for their needs, though more than a third also say they expect the amount budgeted will increase slightly over the next 12 months.

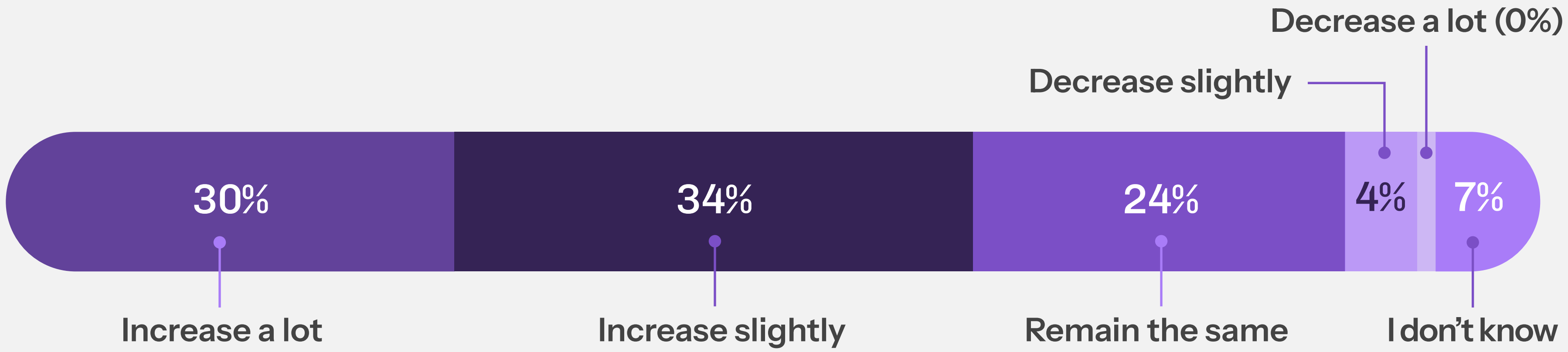
→ Q: What percentage of your IT budget is allocated to cybersecurity?



→ Q: How adequate is your current cybersecurity budget, relative to your organization's needs?



→ Q: How do you anticipate the percentage of your budget allotted to cybersecurity to change over the next 12 months?



Core Quick-Take 01

With IT teams reporting directly to non-technical C-suite roles, **connecting cyber defense to specific business outcomes** is likely to become an increasingly important requirement for securing necessary budgets and staffing.

02 Culture

→ *What's the prevailing cybersecurity mindset, and how does this translate into activities?*

There's a disconnect between prioritizing cybersecurity and taking strategic action.

Nearly two-thirds of respondents say they view cybersecurity as a strategic priority. The data shows, however, that fewer than that say they engage in activities that support this: Only 53% of respondents say they include cybersecurity in their business's ongoing strategic roadmap or factor it into things like partnerships and portfolio decisions (41%) or product development (38%).

→ Q: Which of the following statements best describes the cybersecurity mindset in your organizational culture?

65%

say they consider cybersecurity a strategic priority and business enabler – 35% do not.

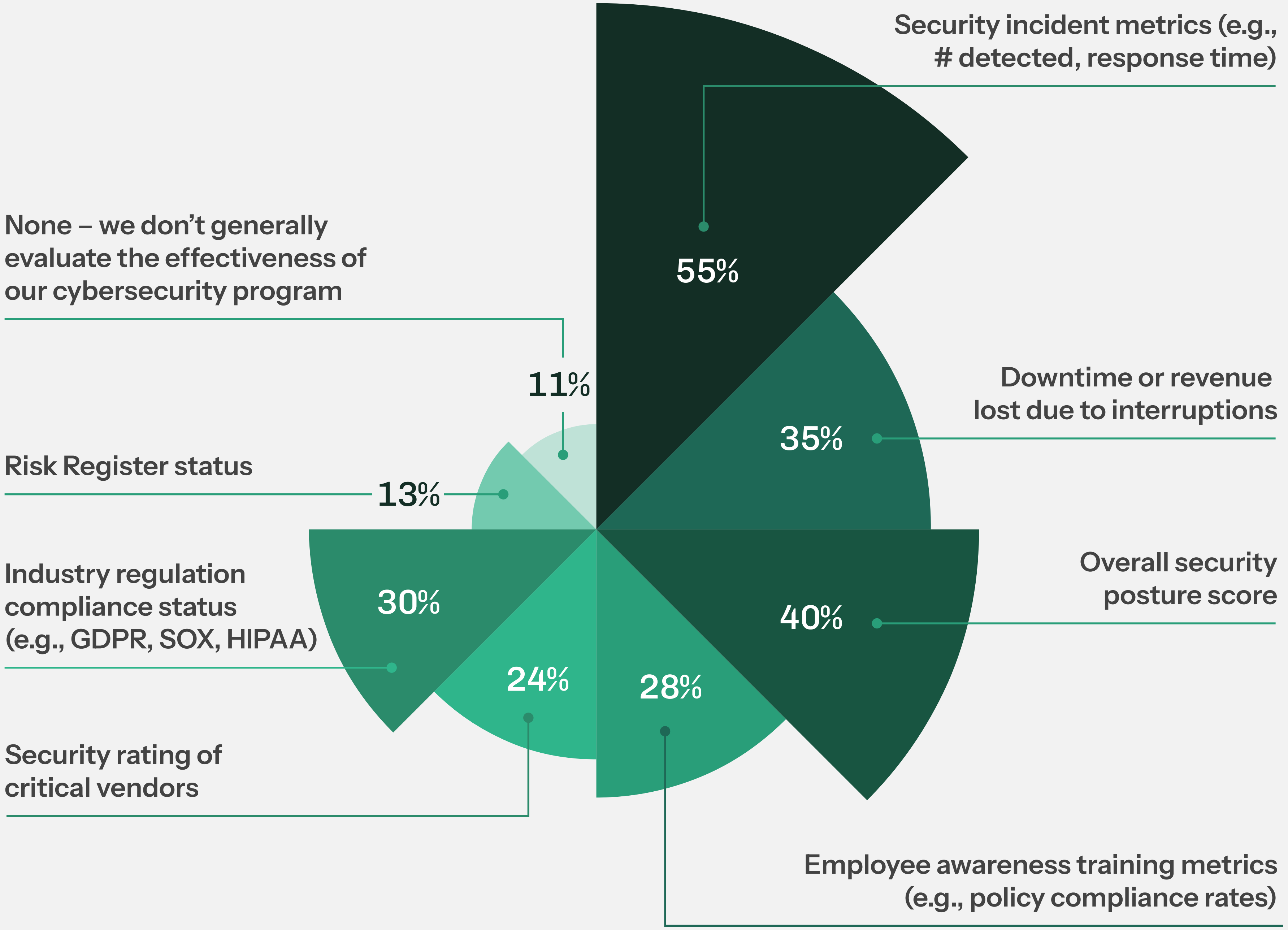
Of those who don't, 25% say it's "more of an IT function than a business function." The rest say it's a "necessary cost center to ensure compliance."

→ Q: Which of the following cybersecurity activities are embedded in your organizational culture? (check all that apply)

53%	We include cybersecurity in our ongoing strategic business roadmap
38%	We factor cybersecurity into all product development stages
41%	We factor cybersecurity into all partnerships and portfolio decisions
27%	We have well thought-out incident response plans
25%	We conduct regular incident response drills
29%	We continuously train employees on cyber awareness
23%	We vet every vendor against rigorous cyber risk criteria
22%	We conduct ongoing due diligence risk assessments on our third-party vendors
17%	We have an IT steering committee that meets regularly
8%	None of the above

From a tactical standpoint, survey participants say they use a variety of metrics to evaluate the effectiveness of their cybersecurity programs, with security incident metrics being the most commonly selected response.

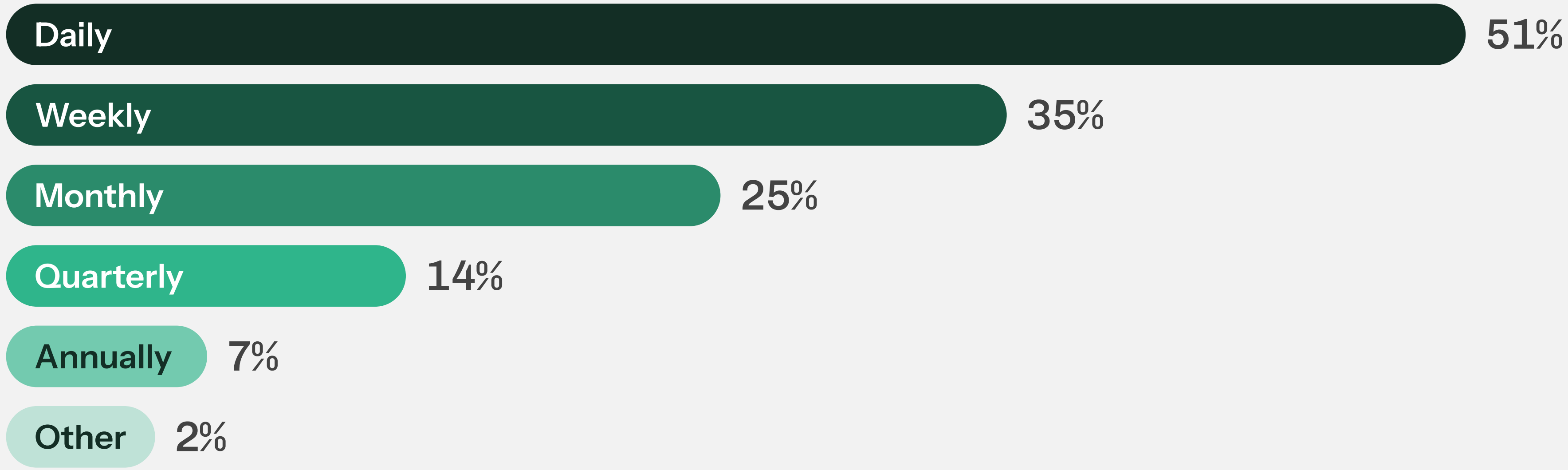
→ Q: Which of the following metrics do you use to evaluate the effectiveness of your cybersecurity program? (check all that apply)



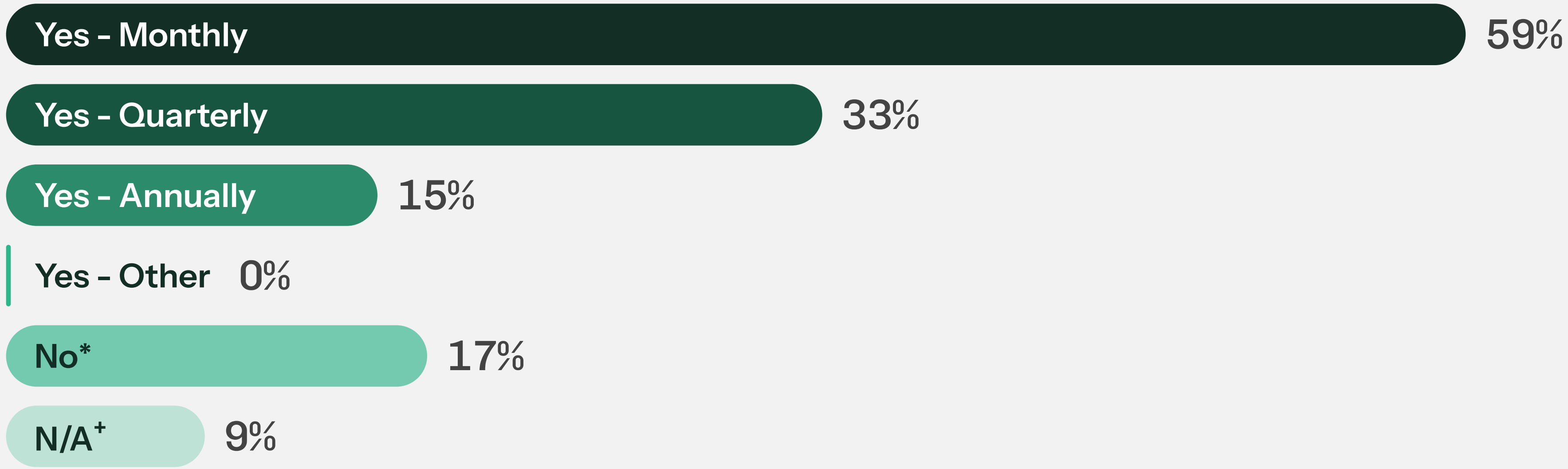
How many different cybersecurity assessment metrics are reviewed and whether they're proactive or reactive, quantitative or qualitative, seem likely to be influencing how the company's cyber posture narrative is being shaped and communicated at the C-suite level.

Most respondents say that updates on the status of their cybersecurity protection are being shared on a frequent basis – daily with executive leadership (51%) and monthly with their board of directors (59%).

→ Q: How frequently is your executive leadership updated on the current level and business impact of cyber risks to your organization? (check all that apply)



→ Q: Are you expected to report on these risks to your board of directors, and if so, how frequently? (check all that apply)



*Our board doesn't require regular cybersecurity risk reports + We don't have a board of directors

Core Quick-Take 02

C-suite executives who don’t consider cybersecurity a strategic priority – or don’t integrate it into their strategic activities – may be focused on the wrong metrics or **undervalue the impact their security posture has on enabling their business goals.**

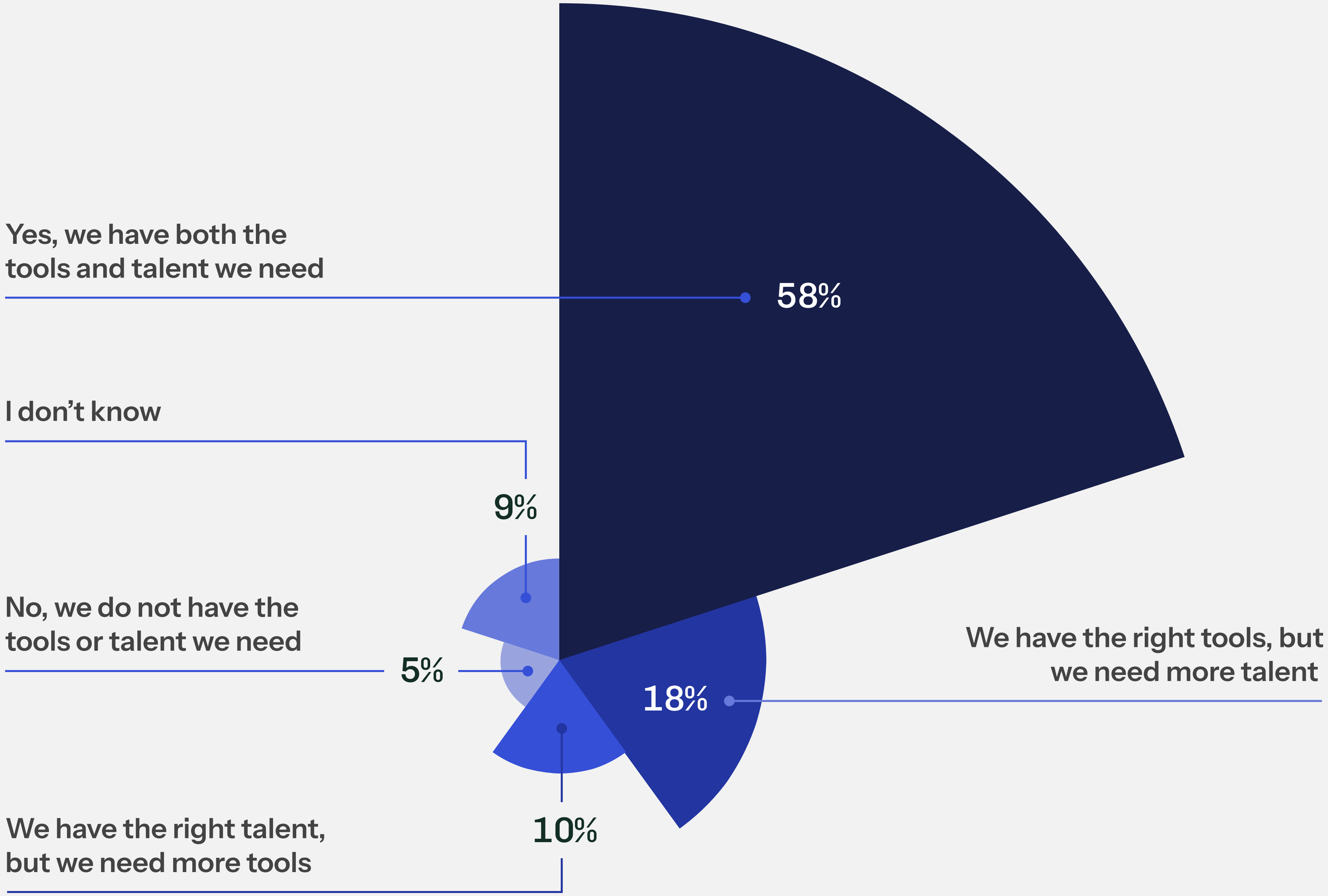
03 Confidence & Skills

→ *How do executives perceive their cyber-preparedness, and what additional skills do they need to develop?*

Leaders express confidence in cyber defenses despite key capabilities gaps.

More than half of survey participants say they have the right cybersecurity tools and talent to mitigate their companies' risk.

→ Q: Do you have the right cybersecurity tools and talent to mitigate risks?



A clear majority also express high degree of certainty that they're doing the right things: 83% say they're extremely confident or confident in their cybersecurity resources' ability to protect their organizations from threats, and 82% say they're extremely confident or confident that their cybersecurity efforts align with those of their industry peers.

→ Q: How confident are you in your cybersecurity resources' ability to protect your organization from threats?

83%

say they're extremely confident (53%) or confident (30%) in their cybersecurity protection.

Only 4% say they're "not at all confident" in their cybersecurity resources' ability to protect their company from threats.

→ Q: How confident are you that your cybersecurity program and practices align with those of your industry peers?

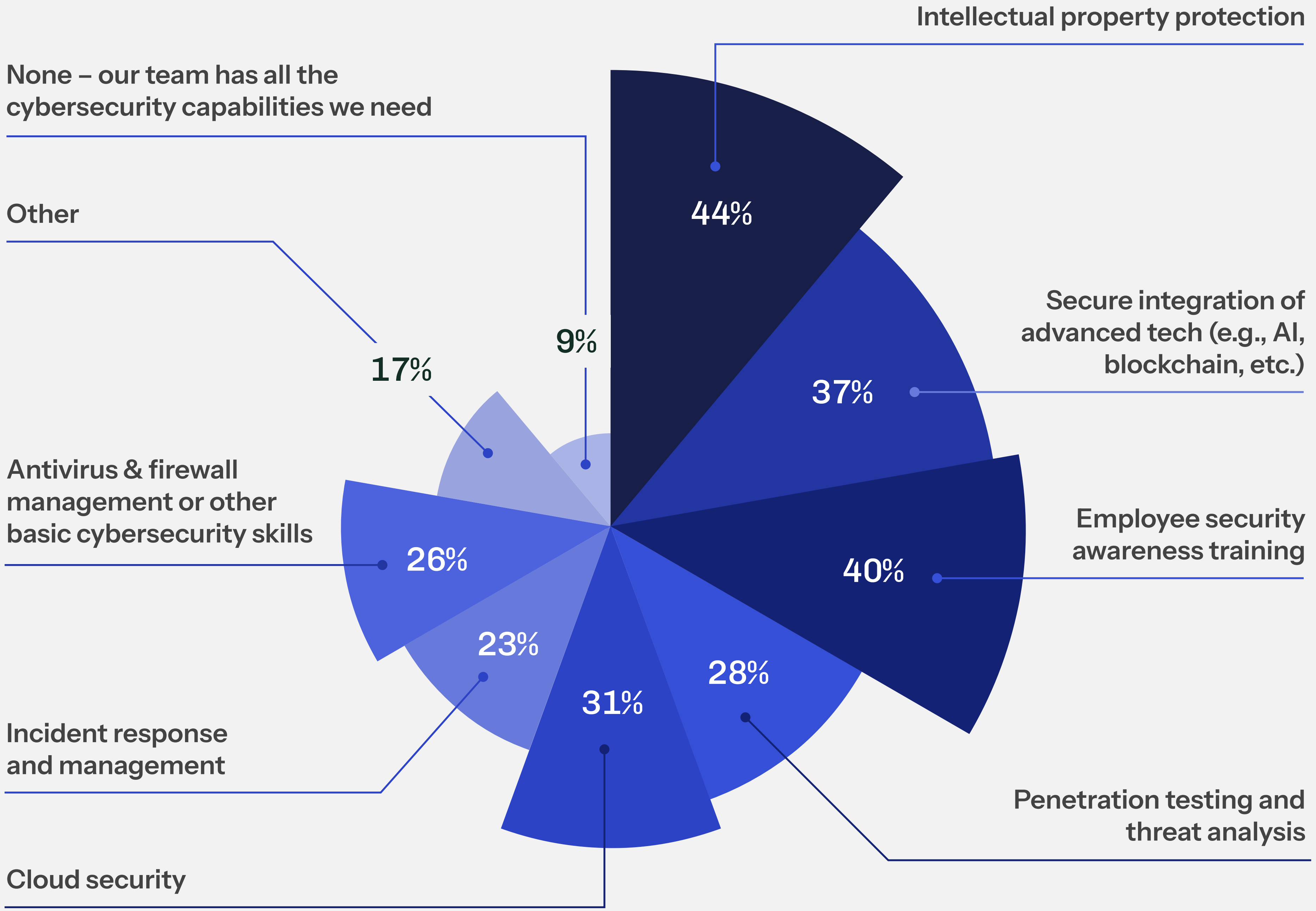
82%

say they're extremely confident (56%) or confident (26%) that their cybersecurity efforts align with those of their industry peers.

Only 3% say they're "not at all confident" they're keeping up with their peers' cybersecurity practices.

When asked to identify any skills gaps in their cybersecurity teams, however, concerns emerge around critical capabilities like intellectual property protection (44%), employee awareness training (40%), and secure integration of advanced technologies like AI and blockchain (37%).

→ Q: Which of the following skills gaps does your organization's cybersecurity team face? (check all that apply)



Core Quick-Take 03

Executives' confidence in their companies' cybersecurity posture doesn't necessarily reflect their teams' existing areas of expertise, **which should raise flags around blindspots and capabilities.**

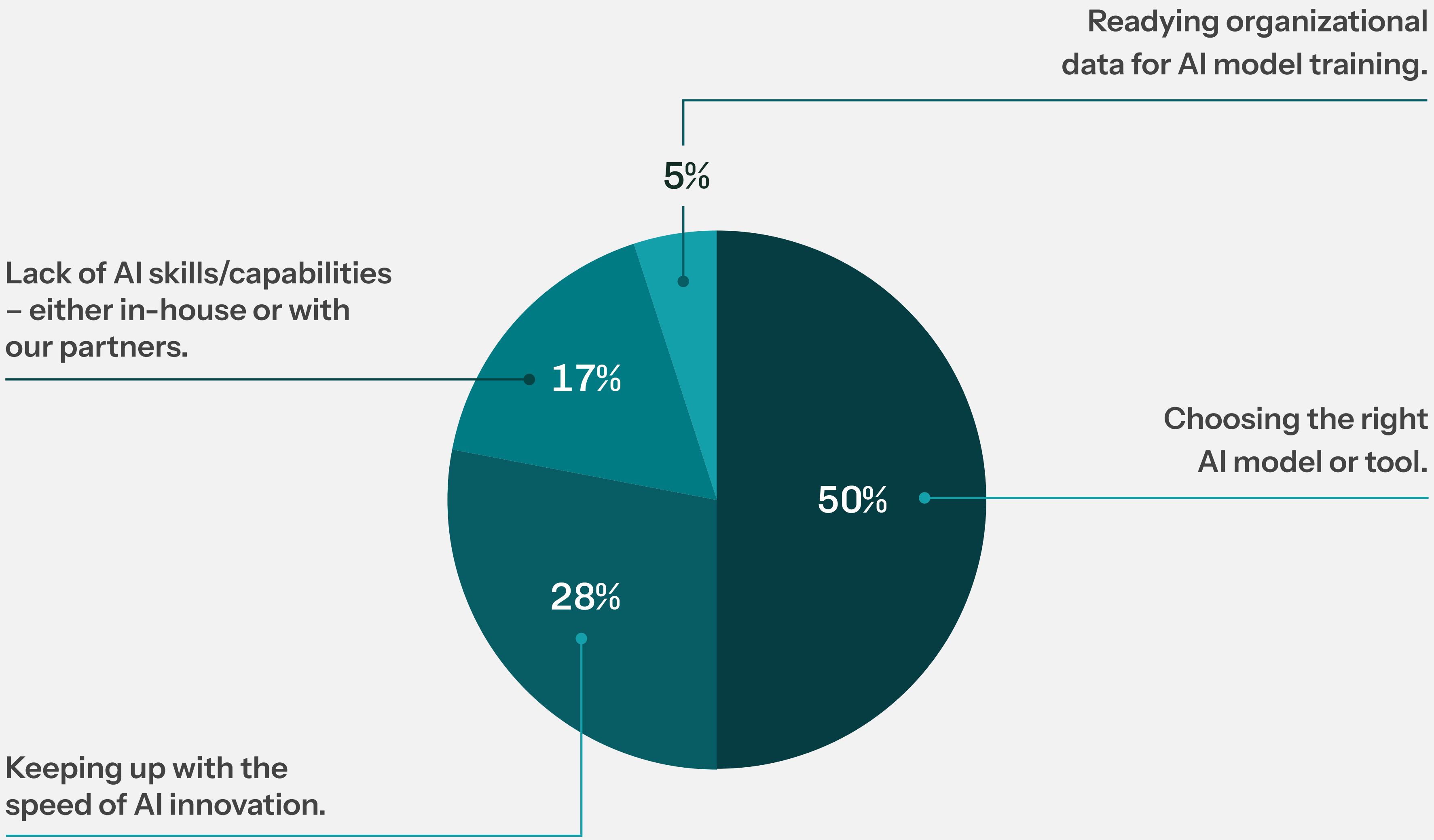
04 AI & Emerging Tech

⟶ *Who's using AI for cybersecurity and compliance, and what else is on their AI to-do lists?*

Cybersecurity emerges as a leading mid-market AI use case.

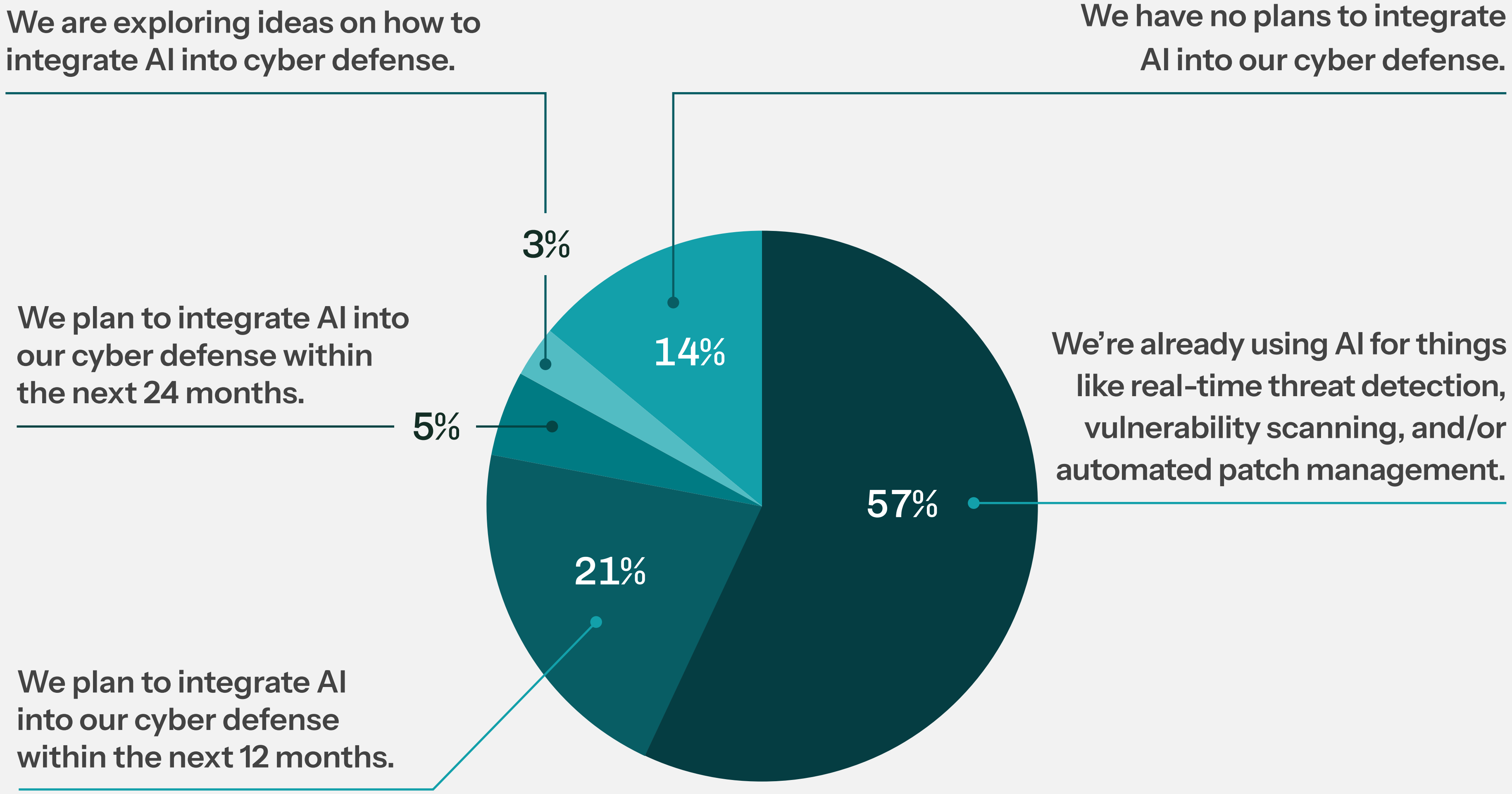
Asked about the biggest AI challenge they face, nearly twice as many respondents selected “choosing the right AI model” over “keeping up with the speed of AI innovation,” a result that seems to be a positive indicator of mid-market companies’ openness to using the emerging technology.

→ Q: With regard to implementing AI in general, which of the following statements best reflects your organization’s biggest challenge?



Indeed, 57% of survey participants overall say they've already incorporated AI into their cybersecurity defense.

Q: With regard to deploying AI as part of your organization's cyber defense, which of the following statements best describes your plans?



From an industry-specific perspective, compliance and risk management are among the top three cited AI use cases across both of the groups focused on in this survey – with 69% of healthcare and life sciences respondents saying they've already implemented it or are in the process of implementing it, and 67% of financial services respondents saying they've already implemented it or are in the process of implementing it.

→ Q: Please share your level of interest/intent with regard to each of the following AI use cases.

Top Healthcare & Life Sciences AI Use Cases 🔒 Cybersecurity related

	Enhancing research and development	Drug discovery and development	Regulatory compliance and pharmacovigilance
Implemented	53%	50%	42%
In Progress	19%	22%	27%
Exploring	13%	8%	16%
Not Interested	7%	12%	9%
Not Applicable	8%	8%	6%

Top Financial Services AI Use Cases 🔒 Cybersecurity related

	Investment screening and analysis & portfolio optimization	Operational efficiency and streamlining back-office productivity	Risk management and compliance
Implemented	44%	36%	37%
In Progress	24%	25%	30%
Exploring	23%	27%	20%
Not Interested	6%	10%	11%
Not Applicable	3%	2%	2%

Core Quick-Take 04

Organizations see AI as a cybersecurity opportunity – with a majority acknowledging that ignoring it entirely isn’t an option.

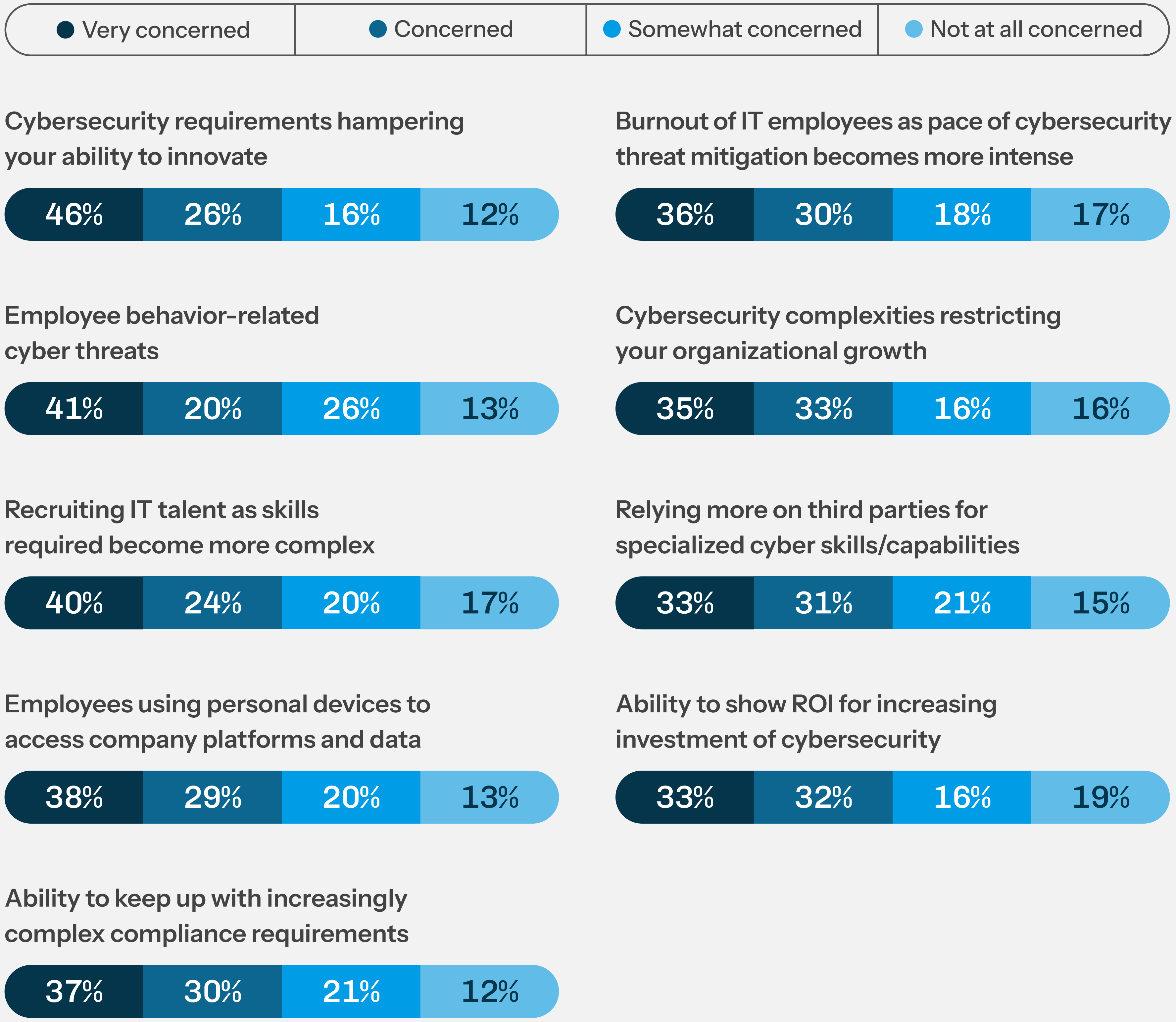
→ *What business areas do leaders worry about cybersecurity requirements disrupting most?*

Innovation and employee-related issues top executives' lists of cybersecurity concerns.

Survey data indicates that for mid-market executives, the long standing tension between wanting to move fast and grow the business while protecting it at the same time is alive and well: Nearly half of participants say they're very concerned about cybersecurity requirements hampering their ability to innovate.

Respondents also share high levels of cybersecurity concern around employees – both in terms of the vulnerabilities they pose and the need to recruit highly skilled IT talent to handle its complex requirements.

→ Q: For each of the following, how concerned are you about the impact it may have on the future of your organization?



Core Quick-Take 05

Some level of concern over cyber protections interfering with innovation (or curtailing growth or compromising compliance and so on) may not be a bad thing if it means C-suite leaders have a **healthy appreciation for both the risks and benefits of modern business technology.**

Findings At A Glance

84% say their IT teams report directly to the C-suite — 67% to the CEO or CFO.

Core Quick-Take 01 With IT teams reporting directly to non-technical C-suite roles, connecting cyber defense to specific business outcomes is likely to become an increasingly important requirement for securing necessary budgets and staffing.

65% say they consider cybersecurity a strategic priority and business enabler — 35% do not.

Core Quick-Take 02 C-suite executives who don't consider cybersecurity a strategic priority – or don't integrate it into their strategic activities – may be focused on the wrong metrics or undervalue the impact their cyber posture has on enabling their business goals.

83% say they're extremely confident or confident in their cybersecurity protection, yet 44% cite gaps in intellectual property protection capabilities.

Core Quick-Take 03 Executives' confidence in their companies' cybersecurity posture doesn't necessarily reflect their teams' existing areas of expertise, which should raise flags around blindspots and capabilities.

57% are already using AI in their cybersecurity.

Core Quick-Take 04 C-suite executives see AI as a cybersecurity opportunity – with a majority acknowledging that ignoring it entirely isn't an option.

46% are very concerned about cybersecurity hampering their ability to innovate.

Core Quick-Take 05 Some level of concern over cyber protections interfering with innovation (or curtailing growth or compromising compliance and so on) may not be a bad thing if it means C-suite leaders have a healthy appreciation for both the risks and benefits of modern business technology.

Survey Methodology

In August 2024, we contracted an independent survey organization to reach out to senior professionals at mid-market companies in the United States. In total, 210 individuals took part in our survey. This data breaks down the demographics of respondents.

Company Size

- **17%** 1–10
- **10%** 1–50
- **20%** 51–100
- **20%** 101–300
- **18%** 301–500
- **6%** 501–1,000
- **4%** 1,000+

Industry

- **50%** Financial Services
- **50%** Healthcare & Life Sciences

Title/Role

- **57%** CEO
- **8%** CFO
- **5%** COO
- **2%** CTO
- **2%** CIO
- **2%** CISO
- **9%** Executive/VP
- **15%** Director/Other

Sector

Financial Services

- **41%** Banking and/or Credit Union
- 15% Asset Management and/or Investment Services
- **6%** Credit & Payment Services
- **20%** Accounting & Tax Services
- **8%** Alternative Investments
- **8%** Investment Banking
- **4%** Other

Healthcare & Life Sciences

- **74%** Hospitals & Healthcare Services
- **2%** Medical Equipment & Devices
- **5%** Health Insurance & Managed Care
- **3%** Healthcare Technology
- **5%** Healthcare Distribution & Retail
- **6%** Wellness & Prevention
- **1%** Education & Training
- **1%** Biotech & Pharma
- **4%** Other

coretelligent

About Coretelligent

We're the business partner you can trust with every facet of your technology. Our expertise is grounded in providing superlative managed IT support but also includes advanced capabilities in cyber security, compliance, data analytics, and workflow automation. From aligning your tech strategy to your business goals to planning and managing your cloud transformation, our engineers have the skills and experience you can count on.

Visit us online at Core.tech →