

2023 Global Chief Information Security Officer (CISO) Survey



Contents

A message from the authors	3
Introduction	4
A look at this year's respondent profiles	6
What CISOs do all day: Reporting lines and remit	11
A material talent risk: A lack of succession planning	17
Risk: Personal, professional, and organizational	18
What's next for CISOs?	23
The state of CISO compensation	26
CISO compensation: United States	27
CISO compensation: Europe	34
CISO compensation: Australia	35

A message from the authors

Welcome to our *2023 Global Chief Information Security Officer (CISO) Survey*, which examines both organizational structure and compensation for this critical enterprise leadership role.

For this report, Heidrick & Struggles compiled organizational and compensation data from a survey fielded in early 2023 of 262 CISOs around the world. Most carried the title of chief information security officer, but respondents also include chief security officers and senior information security executives.

This report includes organizational data from respondents in the United States, Europe, and Asia Pacific, and compensation data for respondents in the United States, Europe, and Australia. We always aim to broaden the spread of our geographical data set and will continue to in the future.

We hope you enjoy reading the report, which is now in its fourth year and widely recognized as the most authoritative and widely disseminated survey of its kind. As always, suggestions are welcome, so please feel free to contact us—or your Heidrick & Struggles representative—with questions and comments.

With warmest regards,



Matt Aiello

Partner

maiello@heidrick.com



Scott Thompson

Partner

sthompson@heidrick.com

Methodology

In an online survey, we asked participants to provide information on how their role is structured, to whom they report and who reports to them, and data on compensation including current base salary, bonus for the most recent fiscal year, and annualized equity or long-term incentive pay, as well as joining bonuses. All data collected was self-reported by information security professionals and has been aggregated.

On confidentiality

The global chief information security officer survey, 2023, has been conducted on an anonymous basis. All data is reported anonymously and in aggregate.

Acknowledgments

The authors wish to thank all those who participated in this survey.

Introduction

The theme of this year's survey of chief information security officers (CISOs) is "more." More risk, more opportunity, more compensation. Even in the context of a cooling hiring market, the role of the CISO is maturing along with the function as organizations' technological needs and risks advance, bringing greater emphasis on cybersecurity. Organizations and leaders must look to the future of the function, ensuring success and continued organizational sustainability with a robust succession plan, expanded cybersecurity expertise and leadership development, and competitive compensation packages.

Respondents this year cited a number of ongoing threats to organizational cybersecurity—risks both personal and organizational, including advancements in artificial intelligence and machine learning, geopolitical risks, and cyberattacks, which include nation/state attacks. "It feels as if cybersecurity threats, both criminal and state-sponsored, [will] continue evolving at a rapid pace that's often unpredictable or surprising," wrote one respondent.

"Systemic risk will increase due to widescale dependence on a few providers," said another. And, said a third: "[There is risk in] less owned infrastructure and more cloud-native assets. Also, skills don't scale from old to new."

We believe that this expertise is more and more crucial not only within organizations and executive teams but on boards as well. However, where there is a need for expertise there is inherent risk—talent risk. A notable 41% of respondents said their company does not have a succession plan in place for the CISO role. Organizations must ensure that they are prepared for the future in the case of a CISO's unexpected departure.

In 2023, the share of CISOs who sit on a corporate board more than doubled, but still remains relatively low, and other Heidrick & Struggles research shows that the addition of board members with cybersecurity skills remains low as well. In the United States, new Securities and Exchange Commission

(SEC) guidance may soon ask public companies to disclose which board members, if any, have cybersecurity experience, thus elevating the role even further. That said, the topic of who is qualified to be a cyber expert on a board remains complex.

As in prior years, the majority of respondents were men, and, in the United States, the majority were also white. Heidrick & Struggles' experience recruiting CISOs so far in 2023 reflects an increasing need for diverse talent. Heidrick & Struggles is proud to share that non-white executives account for 46% of our cybersecurity search placements.¹ We are seeing companies increasingly think outside the traditional industry- and IT-specific criteria for CISOs to find the best executives for the role, including people who are diverse in terms of gender and race or ethnicity, as well as industry and functional expertise.

1 Heidrick & Struggles' proprietary data.

Key findings

Organizational structure and risks

- Forty percent of CISOs reported that their company does not have a succession plan for the role; 13% said their company isn't in the process of developing one.
- This is particularly concerning considering the importance of the role. Among leaders, according to a recent survey we conducted, 76% said they were very or entirely open to changing companies in the next three years.² A lack of succession planning should be considered an organizational risk.
- Unsurprisingly, AI is the most often identified significant threat in the next five years. It's one of many threats that will require a constant and rapid evolution of the CISO's skills and is part of a broader trend of the CISO role becoming more technical. Specifically, we are seeing a rise in the need for CISOs to understand software engineering and cloud security. This tracks with the general "shifting left" of security, a trend in which "security measures, focus areas, and implications should occur further to the left—or earlier—in the lifecycle than the typical phases that used to be entry points for security testing and protections."³
- However, the good news is that 80% of respondents agree that they are able to invest in leadership and development to build or enhance team capabilities.
- Over half of respondents say they believe their board only somewhat has or does not at all have the knowledge or expertise to respond effectively to their presentations, but only 30% of CISOs say they currently sit on a corporate board—still a notable leap from the 14% who said the same in the prior year.

Compensation

- As we have seen in past surveys, US CISOs generally report the highest compensation. For CISOs in the United States, reported median total cash compensation increased 6% year over year, to \$620,000 in 2023. Median total compensation, including any annualized equity grants or long-term incentives, also increased, up to \$1,100,000 this year.
- The average total cash compensation for CISOs in Europe was \$457,000. Average total compensation, including any annualized equity grants or long-term incentives, was \$552,000.
- The average total cash compensation for CISOs in Australia was \$368,000. Average total compensation, including any annualized equity grants or long-term incentives, was \$586,000.
- Across regions, CISOs in the financial services industry reported the highest average total compensation, while those in the technology and services industry received the highest average annual equity or long-term incentives (LTI).

² Proprietary data from a survey of 250 executives in six countries around the world conducted in spring 2023.

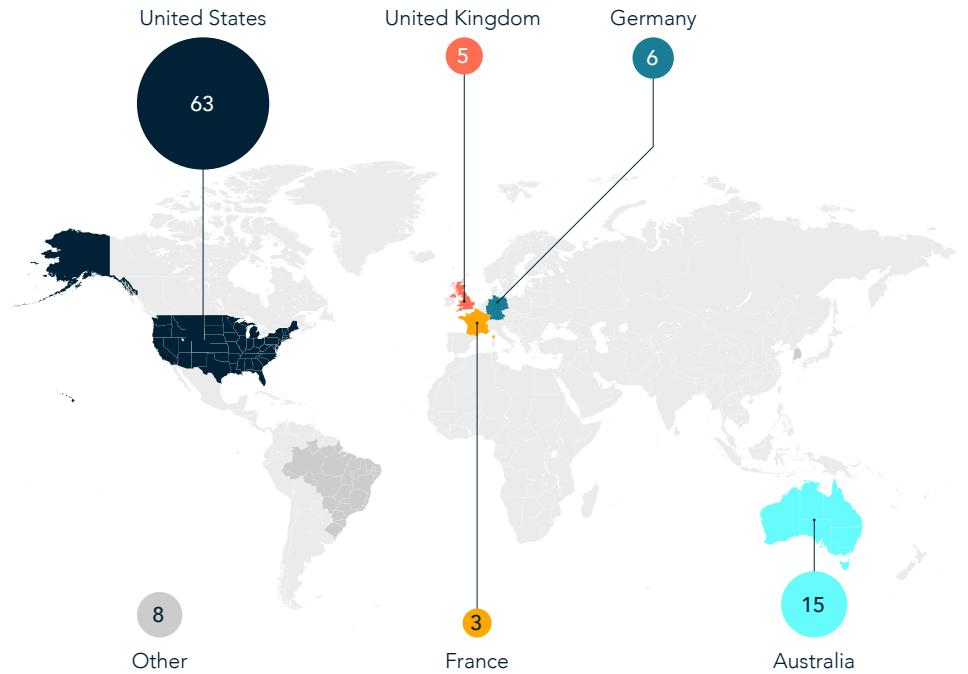
³ Zachary Malone, "What executives should know about shift-left security," CIO, February 24, 2023, cio.com.

A look at this year's respondent profiles

The CISOs who responded to the survey came predominantly from the United States. Australia, France, Germany, and the United Kingdom were also represented.

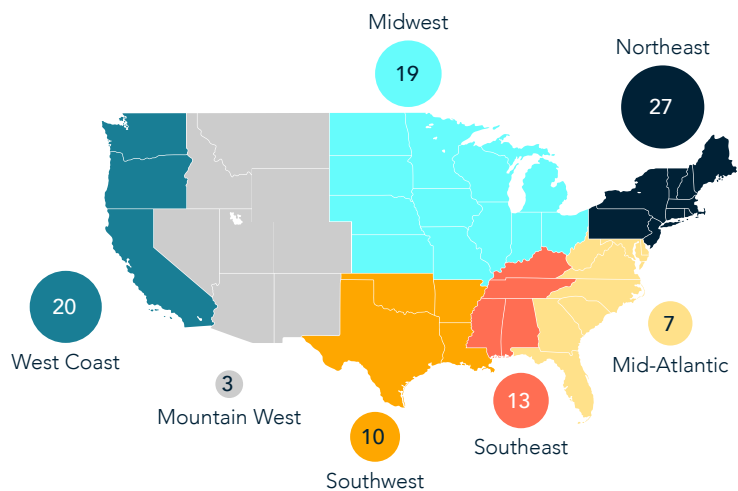
Respondents' location (%)

Country



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 262 information security professionals

US region

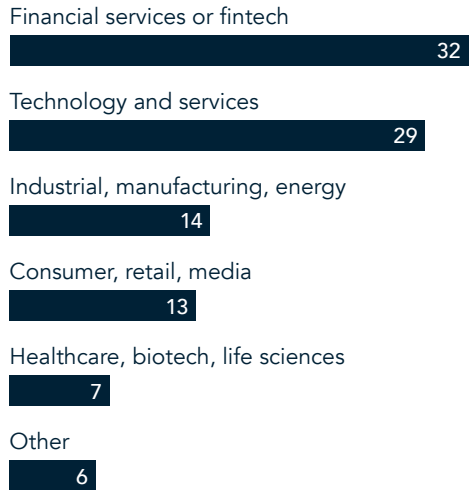


Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 163 information security professionals
 Note: Numbers may not sum to 100%, because of rounding.

More than half of the CISOs were at companies with annual revenue of \$5 billion or more, and they worked across a range of industries, most often financial services and technology and services.

Company information (%)

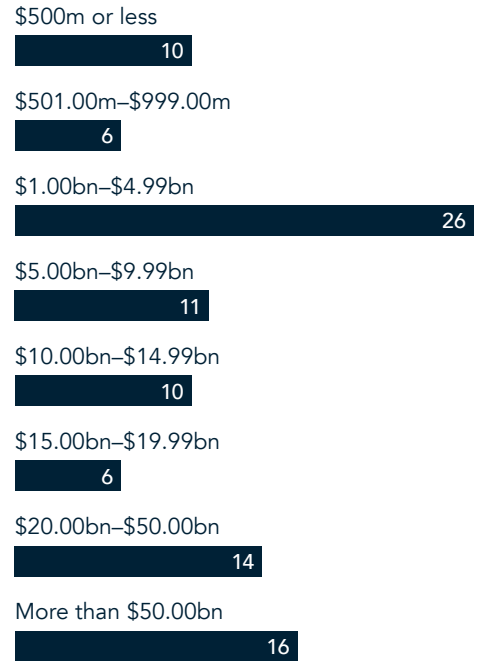
Current company industry



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 244 information security professionals

Note: Numbers may not sum to 100%, because of rounding.

Most recent annual revenue (USD)



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 228 information security professionals

Note: Numbers may not sum to 100%, because of rounding.

In terms of experience, nearly half of CISOs reported having spent the majority of their careers in the technology infrastructure function. We also continue to see the “shift left” in skill set to more technical cyber leaders, notably coming from software engineering. Said one respondent to our survey, “Software development risks (from supply chain to app security, and so on) are increasingly relevant for most CISOs. [The] adoption of

cloud, SaaS, and more effectively managed endpoint systems have reduced the focus on classic IT security management processes.”

Only 1% of CISOs have spent the majority of their careers in compliance, marking the end of regulatory compliance as a viable path to a CISO role.

Respondents in Europe had less often spent the majority of their careers in

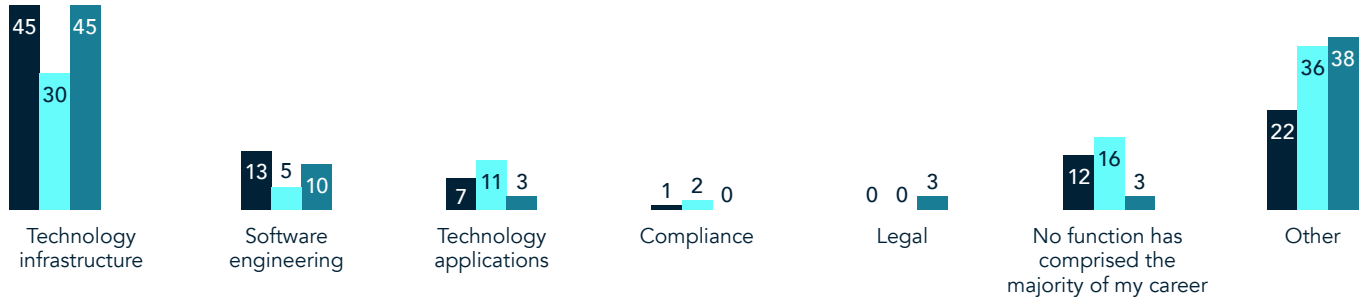
technology infrastructure and more often said they’d spent their time in technology applications, or that no function in particular had comprised the majority of their careers.

Prior to their current role, more than half of the respondents were in another CISO role. This reflects a broader trend that the career path forward for CISOs is most often to another CISO role.

Career experience, by country (%)

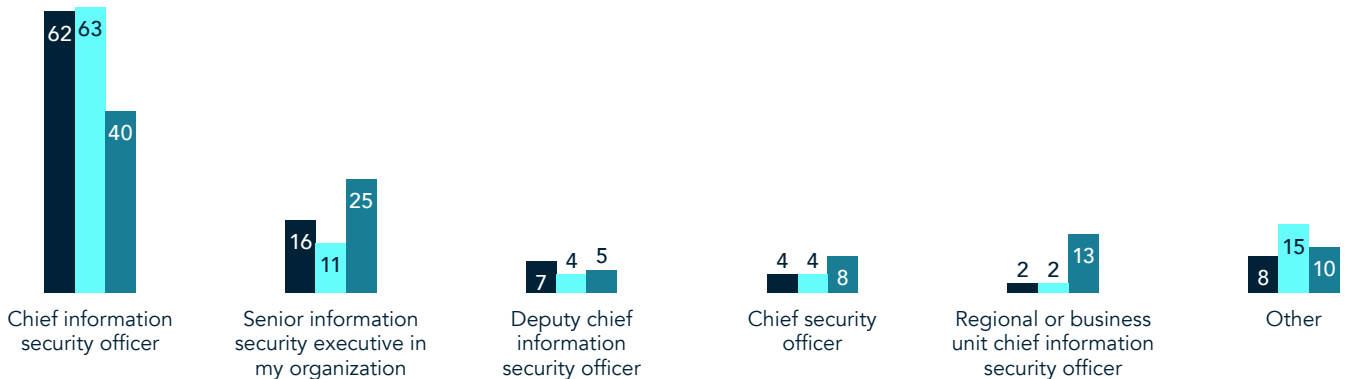
■ United States ■ Europe ■ Australia

Function in which respondents have spent the majority of their career



Source: Heidrick & Struggles’ global chief information security officer (CISO) survey, 2023, n = 249 information security professionals

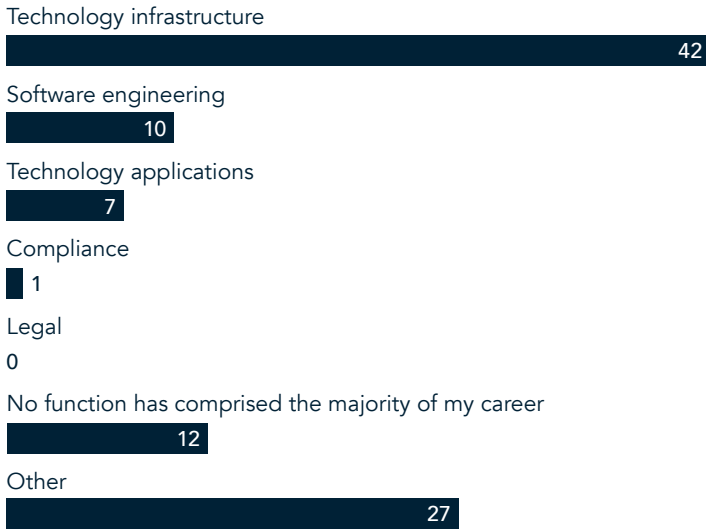
Prior role or function



Source: Heidrick & Struggles’ global chief information security officer (CISO) survey, 2023, n = 250 information security professionals

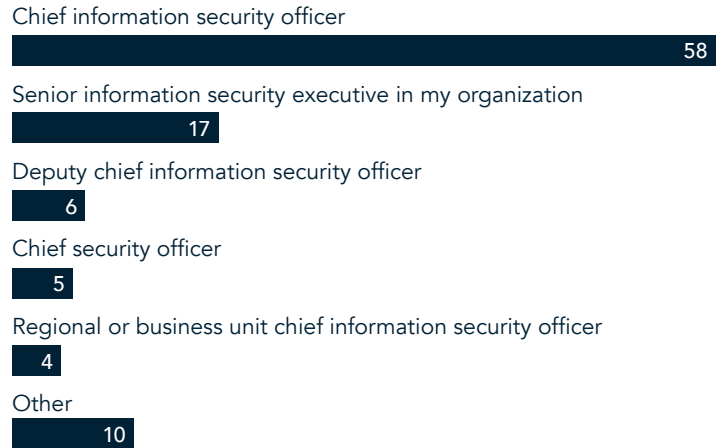
Career experience overall (%)

Function in which respondents have spent the majority of their career



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 259 information security professionals

Prior role or function



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 260 information security professionals

The median tenure of this year's respondents in their current role was four years—the same as last year. Just over half had been in their role for at least three years, down from 77% last year and even slightly below the 56% who said the same in 2021.

We believe CISO tenure has stayed level due to broader macroeconomic uncertainty. When markets open once more, pent-up demand for new challenges will cause more CISO movement.

Current role background (%)

Tenure in current role

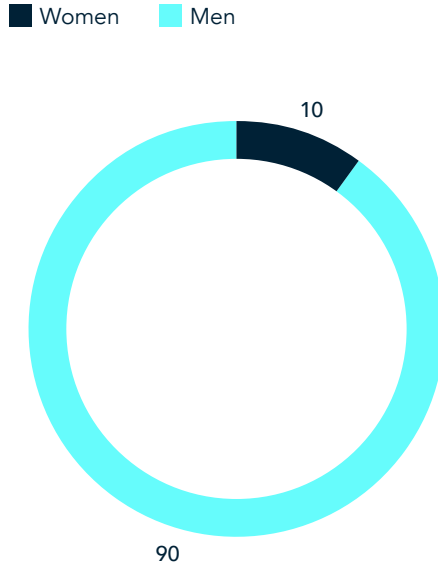


Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 243 information security professionals

Globally, most respondents were male, and, in the United States, most were white. In the United States, the share of non-white respondents rose to 32%, from 22% in 2022. We believe this reflects companies' greater openness to bringing diverse skill sets into the role.

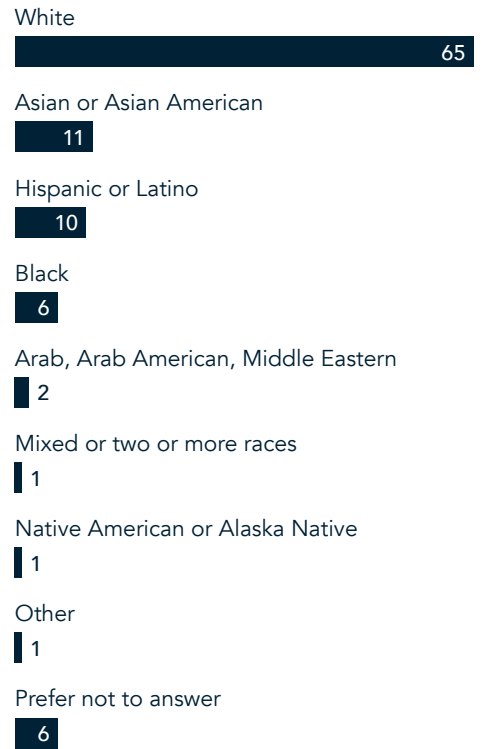
Demographics (%)

Gender



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 229 information security professionals

Race or ethnicity (United States)



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 165 information security professionals

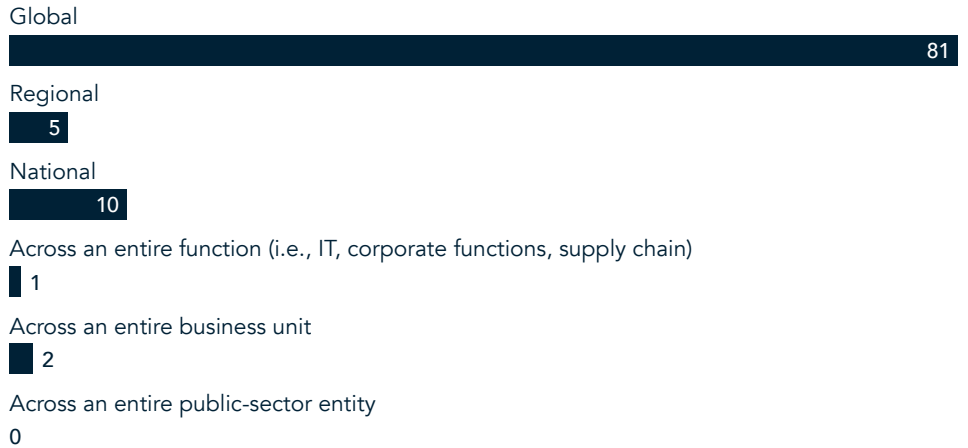
Note: Numbers may not sum to 100%, because of rounding.

What CISOs do all day: Reporting lines and remit

Many respondents cited geopolitical risk as one of the top threats facing them, highlighting the importance of having a person in a global role. However, we suspect that, as the function grows, we will see an emergence of regional CISOs, who will enable organizations building corporate infrastructure in new regions to understand and mitigate region-specific risks.

Current role background (%)

Remit of your role



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 242 information security professionals

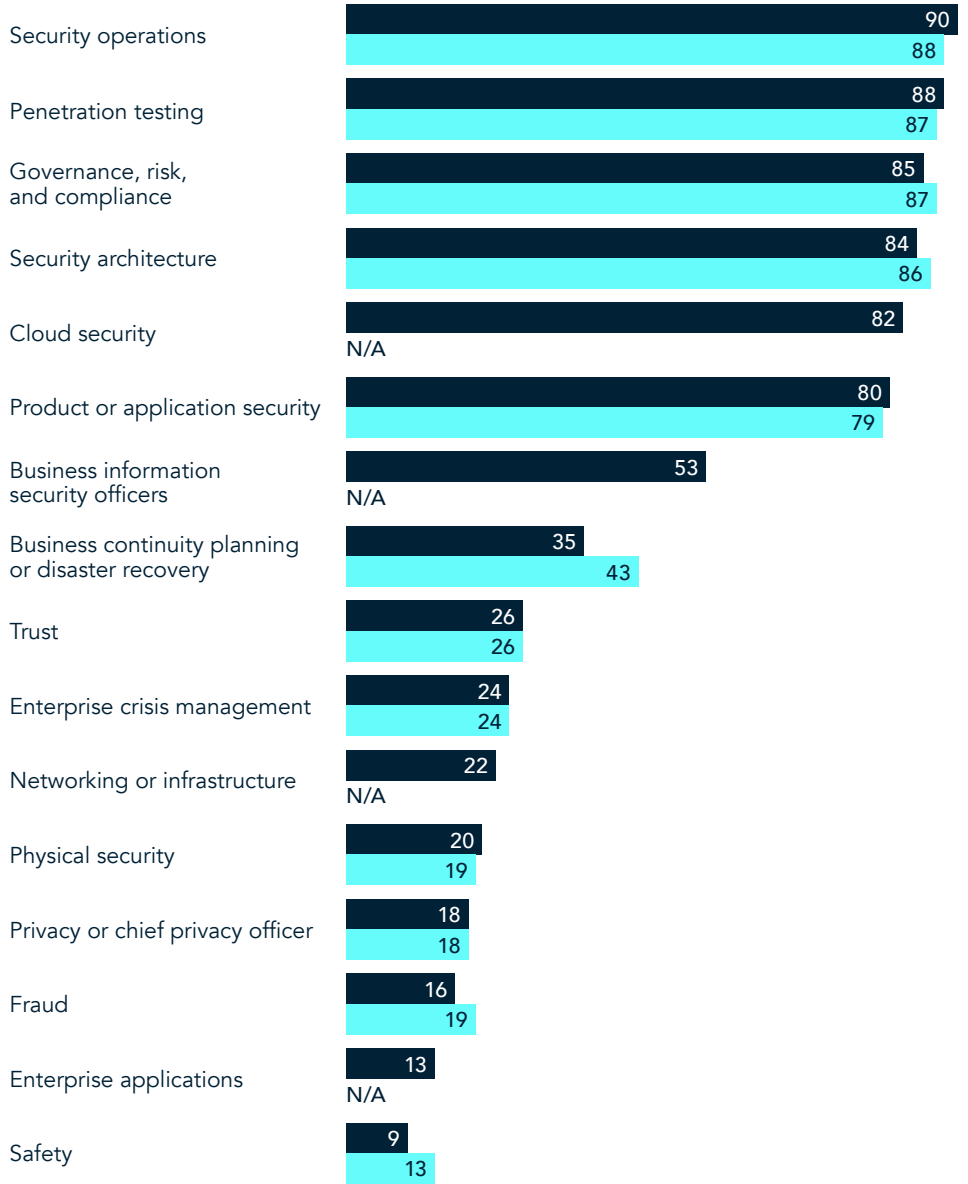
Note: Numbers may not sum to 100%, because of rounding.

The functions that most CISOs say report to them have remained generally the same year over year, with the addition this year of cloud security.

Team information (%)

■ 2023 ■ 2022

Which functional areas report to you?



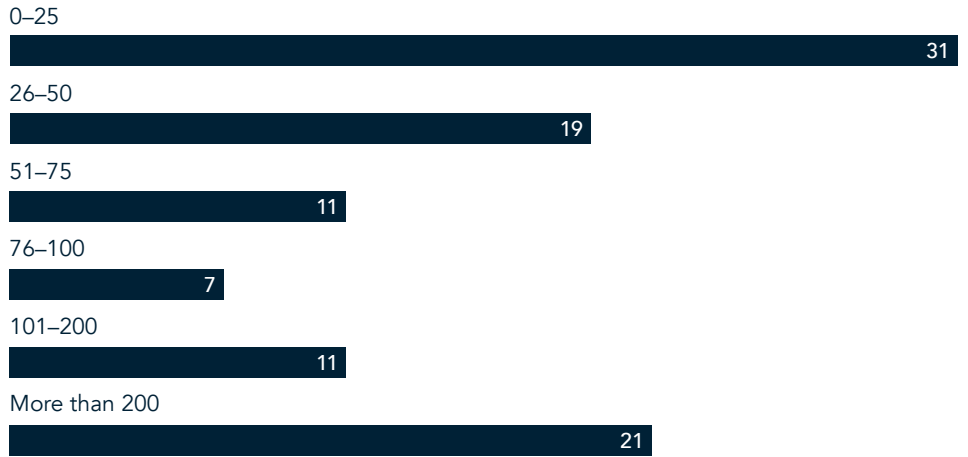
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 240 information security professionals; and Heidrick & Struggles' global chief information security officer (CISO) survey, 2022, n = 327 information security professionals

Those areas of responsibility are aligned with the most significant cybersecurity threats CISOs say their companies are facing (see chart “Most significant cyber risks in five years” on page 17). As previously mentioned, we are seeing cybersecurity becoming more and more embedded in core software development and business processes, with the most sophisticated cyber programs getting ahead of threats and taking a “security by design” approach. As software, AI, and machine learning are becoming ubiquitous even outside technology companies, organizations across industries are recognizing the need to embed security protocols and secure design earlier in software development processes—the shifting left. CISOs must now have the technology acumen to communicate with engineers and developers on a deeper level in order to build robust cybersecurity programs embedded in both their organization’s structure and products.

Team size was, on the whole, similar to that reported last year. Comparing regions, Australian respondents had the smallest teams, while US respondents reported the largest.

Team information (%)

Team size (global)

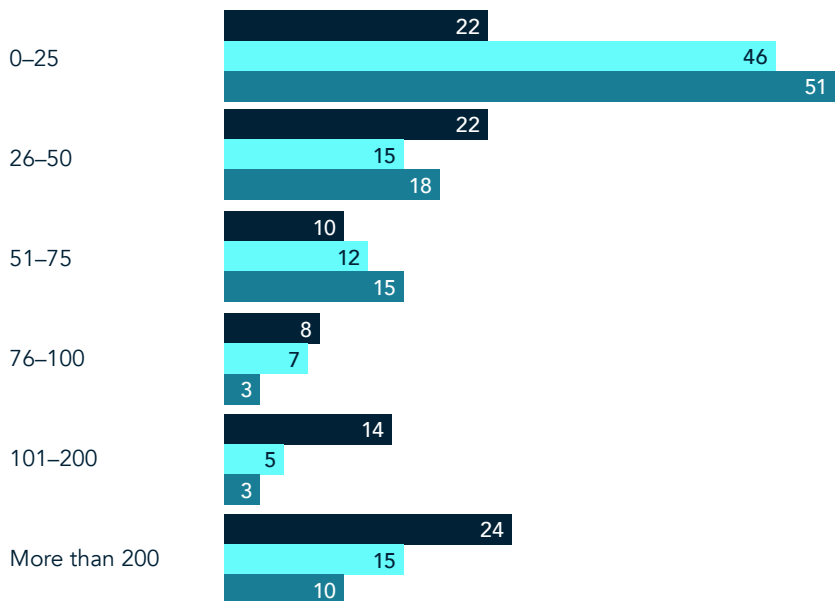


Source: Heidrick & Struggles’ global chief information security officer (CISO) survey, 2023, n = 242 information security professionals

Team size, by country (%)

■ United States ■ Europe ■ Australia

Team size



Source: Heidrick & Struggles’ global chief information security officer (CISO) survey, 2023, n = 234 information security professionals

In terms of their own reporting structure, 5% of respondents report directly to the CEO, a decrease from 8% in 2022 and 11% in 2021. By region, a notable 12% of European respondents report to the CEO, while more than a quarter of the Australian respondents report to the CTO or senior engineering executive.

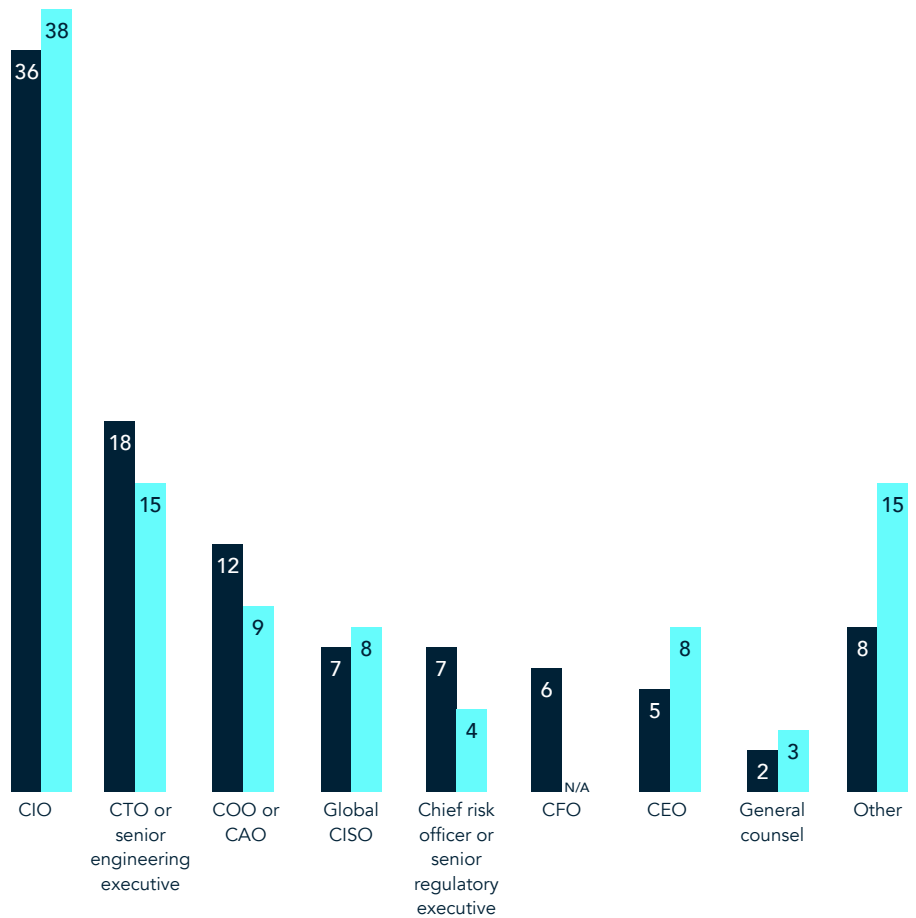
Overall, there was a slight decrease in those who report to the CIO—from 38% in 2022 to 36% in 2023—and slight increases in those who report to the CTO or senior engineering executive and in those who report to the COO or chief administrative officer (CAO). This, again, is indicative of the shifting left of the role, from compliance into technology.

Two-thirds of CISOs are two levels down from the CEO, that is, reporting to a role that reports directly to the CEO. Sixty-four percent report to someone other than the CIO, about the same share as last year. We believe that the number of CISOs reporting to CIOs will continue to decrease as the CISO role takes a broader enterprise risk oversight role with direct ties to the audit committee and board. Anecdotally, we are even seeing CIOs report to CISOs in West Coast technology companies.

Current role background (%)

■ 2023 ■ 2022

To whom respondents report overall

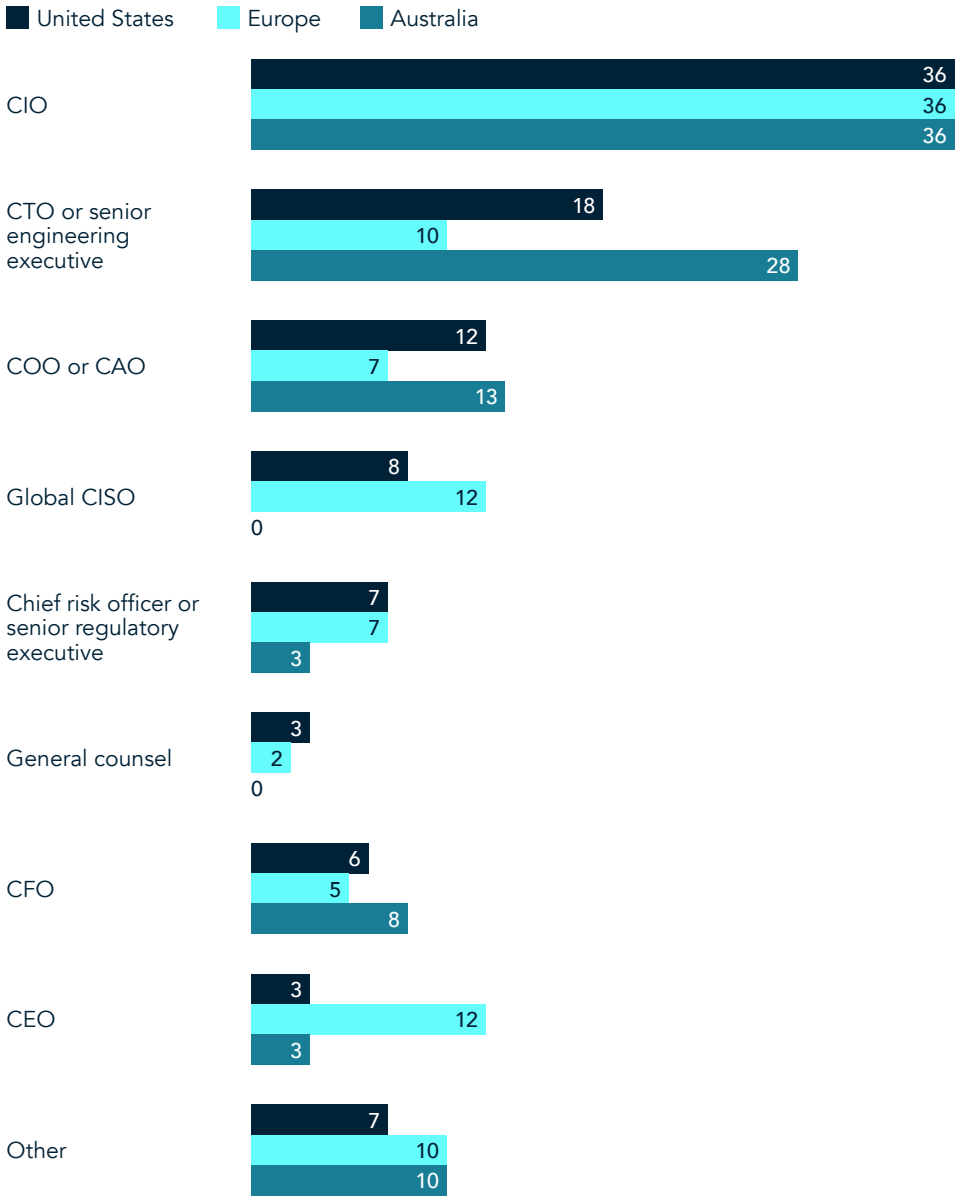


Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 244 information security professionals

Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2022, n = 327 information security professionals

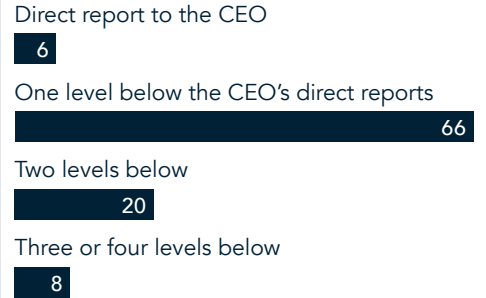
Current role background (%)

To whom respondents report, by country



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 235 information security professionals
 Note: Numbers may not sum to 100%, because of rounding.

Seniority



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 260 information security professionals

CISOs have significant visibility with the board: 91% said they present to the full board or a committee, up from 88% last year. Those who present to the full board most often report annually, while those who present to a special committee such as audit, risk, or technology most often do so quarterly.

Presentations to the board (%)

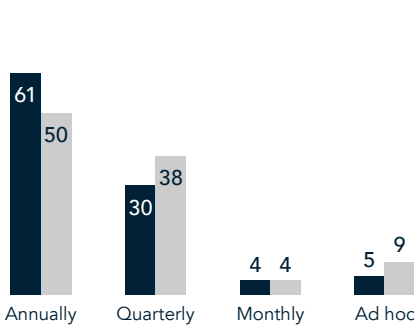
To whom respondents report overall, 2023



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 243 information security professionals; and Heidrick & Struggles' global chief information security officer (CISO) survey, 2022, n = 327 information security professionals

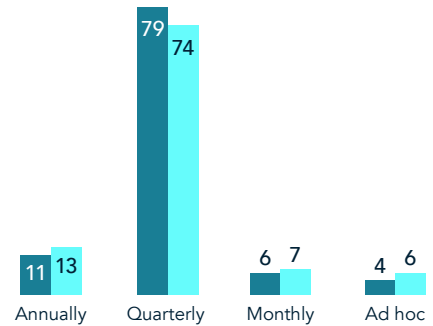
Presentation frequency

Frequency present to full board



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 143 information security professionals
Note: Numbers may not sum to 100%, because of rounding.

Frequency present to committees



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 185 information security professionals

The majority of respondents either agree or strongly agree that they have adequate exposure to the board. However, only slightly less than half of CISOs say that the board has the knowledge or expertise to respond effectively to their presentations (see chart "Attitudes around board exposure and effectiveness" on page 24).

Attitudes around board exposure and effectiveness (%)

I have adequate exposure to the board or board members as needed



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 243 information security professionals

A material talent risk: A lack of succession planning

Forty-one percent of respondents say their company does not have a succession plan in place for the CISO role, though more than half of those that do not have a plan are developing one.

However, of those who claim to have a succession plan, less than half have one that has identified multiple candidates. In our experience, a robust succession plan is, instead, a well-developed leadership pipeline with prospective candidates who can be ready and willing to step up across multiple timeframes.⁴

This lack of succession planning for the CISO role is a serious problem as organizations simply cannot afford to leave the cyber function vacant, for multiple reasons:

- **Threat:** The threat landscape that every company faces today has made lacking a cyber leader

succession plan more than an HR problem. It's now a business issue.

- **Regulatory:** Cyber is a board-level, regulated business risk that is only growing in prevalence. We're increasingly seeing this top of mind for regulators as they inquire about company preparedness in cybersecurity—even requiring regulated firms to have a CISO.
- **Availability:** CISOs are difficult to promote beyond a title or scope increase laterally, making the most likely next step for a CISO another company. It can take significant resources—including time, money, and effort—to replace them.

That leaves the question: how to find the next CISO? The question incorporates a range of factors, including current and future business strategy, regulatory requirements, company culture, marketplace and

compensation trends, and more. The CISO is also a particularly difficult position to replace, given constraints with training an internal candidate in all areas without compromising their day-to-day work, along with ensuring they're ready to engage with the board on an increasingly pertinent topic.⁵

Organizations overall must ensure that CISO succession planning is continually kept alive. It can't be a one-and-done task, out of mind once a successor is chosen. Like CEO succession, the CISO role should be a regular topic of conversation at the highest levels, placing information security strategy and preparedness at the center of the business at all times. Approaching succession proactively in this way will ensure information security strength for years to come.

Company's current plan for the CISO role (%)

We have a succession plan that has identified multiple candidates

24

We have a succession plan with one successor in place

36

We don't currently have a succession plan in place, but are in the process of developing one

28

We don't currently have a succession plan and are not in the process of developing one

13

Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 240 information security professionals

⁴ For more on succession planning, see Cynthia Emrich, Steven Krupp, and Amy Miller, "Developing future-ready leaders: From assessments to strategically aligned learning," Heidrick & Struggles, heidrick.com.

⁵ Matt Aiello and Scott Thompson, "Who will be your next CISO? Plan ahead to make the most of this critical role," LinkedIn, forthcoming on linkedin.com.

Risk: Personal, professional, and organizational

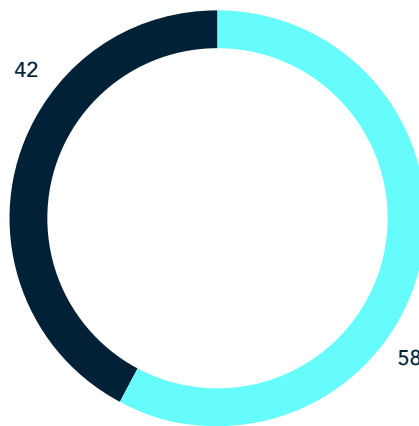
The importance of the role of the chief information security officer continues to grow as digital technologies, particularly artificial intelligence, become even more prevalent and concern about cyberattacks, specifically ransomware, rises.

In that context, we asked again about the risks, both personal and professional, that CISOs face in their role. Unsurprisingly, the most often cited cybersecurity risk was AI and machine learning, followed by geopolitical risks and cyberattacks, which include ransomware, malware, insider threats, and nation/state attacks. And more than half of respondents said they believe that the most significant cyberrisks will not be the same five years from now.

Most significant cyberrisks in five years (%)

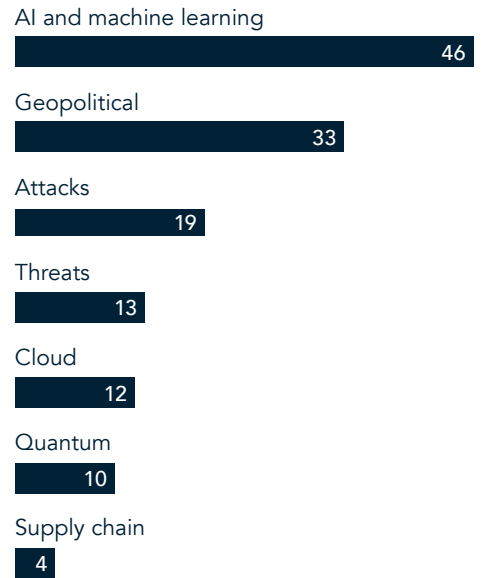
Cyberrisks five years from now

- The risks will be different
- The risks will be mostly the same as they are now



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 241 information security professionals

Top themes in most significant cyberrisks

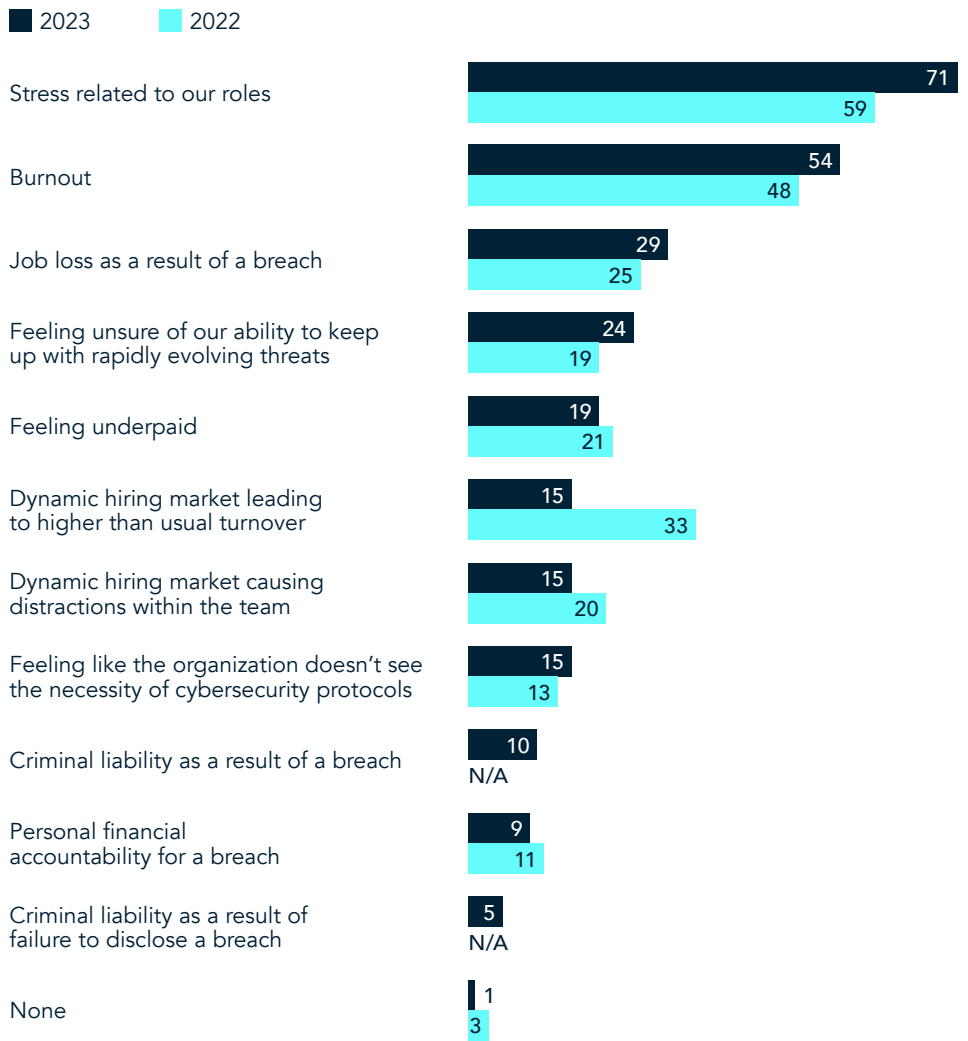


Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 118 information security professionals

Many respondents added additional thoughts this year on this topic. There will be “a continued arms race for automation,” one respondent wrote. “As attackers increase [the] attack cycle, respondents must move faster.” “Cyber threats [will be] at machine speed, whereas defenses will be at human speed,” wrote another. Others expressed similar concerns, that skills will not scale from old to new. Still others had more existential fears, citing the “dramatic erosion in our ability to discern truth from fiction.”

In terms of personal risks, stress and burnout remain top concerns, growing year over year. There was also a small increase in concern about the ability to keep up with rapidly evolving threats as well as job loss as a result of a breach, up to 29% from 25% in 2022.

Most significant personal risks you face in your role (%)



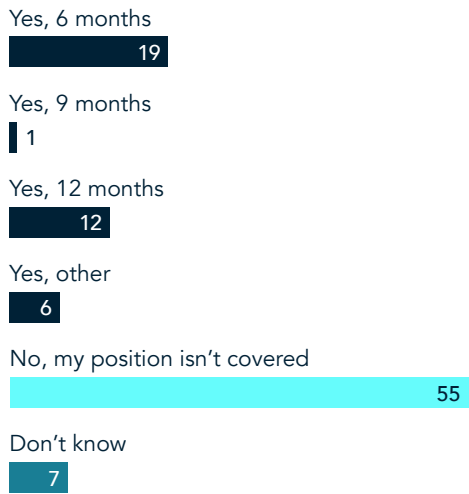
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 241 information security professionals; and Heidrick & Struggles' global chief information security officer (CISO) survey, 2022, n = 327 information security professionals

This is notable because 55% of respondents are in a position that is not covered by a severance agreement, and 38% are not covered by directors and officers (D&O) insurance (18% do not know). However, while severance agreements are comparable across regions, D&O insurance coverage varies significantly. While 34% of US respondents are not covered by D&O insurance, 45% of European respondents are not covered, nor are 51% of Australian respondents.

The best-positioned CISOs should be able to command executive-level protections that enable them to do their jobs unencumbered by the threat of career risk.

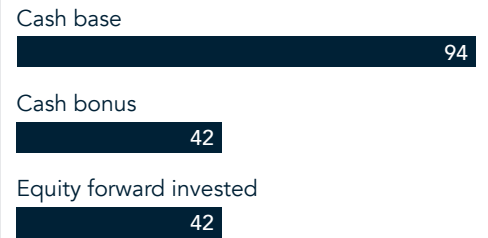
Position severance policies and D&O insurance, global (%)

Position covered by a severance agreement



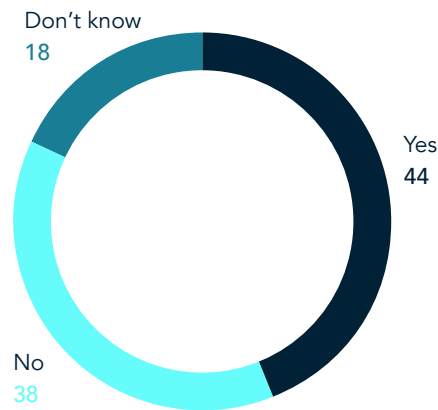
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 234 information security professionals

What's covered in severance policy



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 85 information security professionals

Position covered by D&O insurance (%)

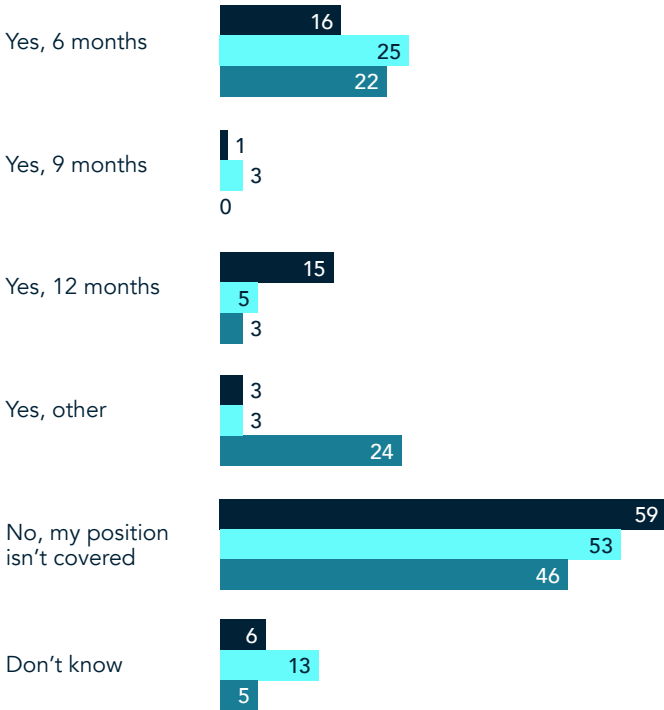


Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 236 information security professionals

Position severance policies and D&O insurance, by country (%)

United States Europe Australia

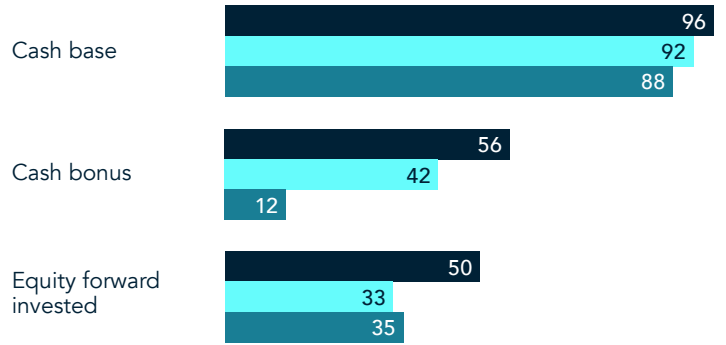
Position covered by a severance agreement



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 148 information security professionals in the United States; Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 40 information security professionals in Europe; and Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 37 information security professionals in Australia

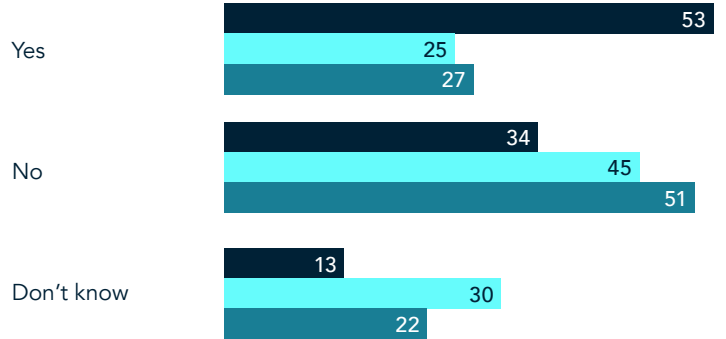
Note: Numbers may not sum to 100%, because of rounding.

What's covered in severance policy



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 52 information security professionals in the United States; Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 12 information security professionals in Europe; and Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 17 information security professionals in Australia

Position covered by D&O insurance



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 150 information security professionals in the United States; Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 40 information security professionals in Europe; and Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 37 information security professionals in Australia

The good news is that CISOs generally agree that they receive adequate support regarding enterprise risk: they have the funding and executive support to build the necessary security program, cybersecurity is included in their organization's business strategy, they can attract the talent they need, and they are able to invest in learning and development to build team capabilities.

Share of respondents who either agree or strongly agree with the following statements... (%)

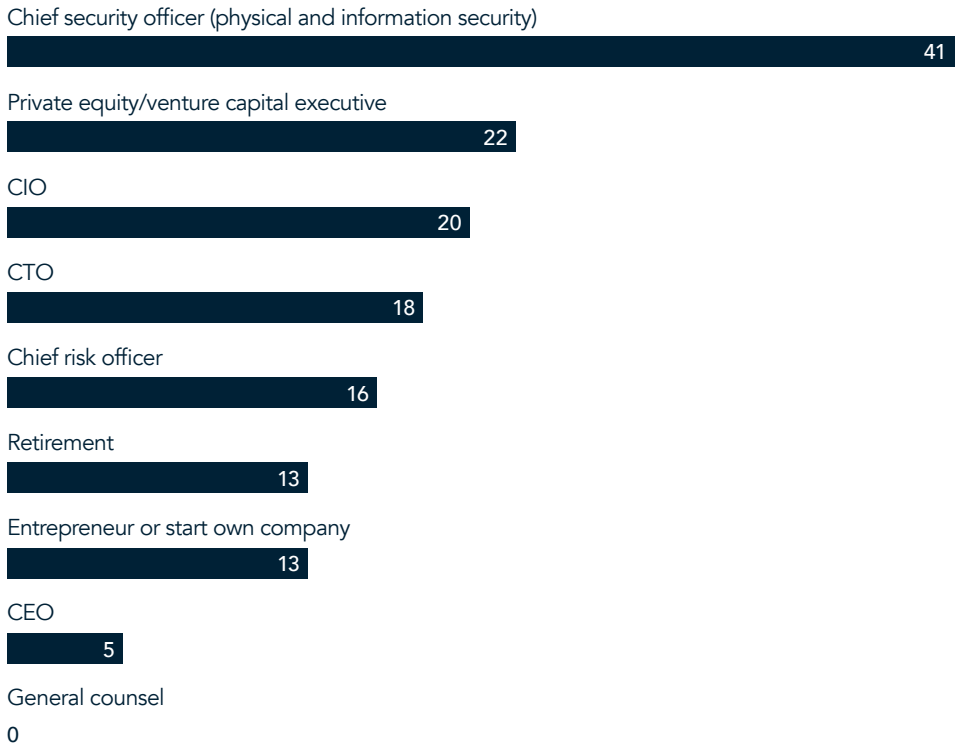


Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 243 information security professionals

What's next for CISOs?

In the context of so many CISOs coming to their current role from a former CISO role, we are increasingly interested in the question of where CISOs want to go next. A majority do want to be something other than a CISO, such as a private equity or venture capital executive, a chief information officer, or a chief technology officer.

Ideal next executive role (%)

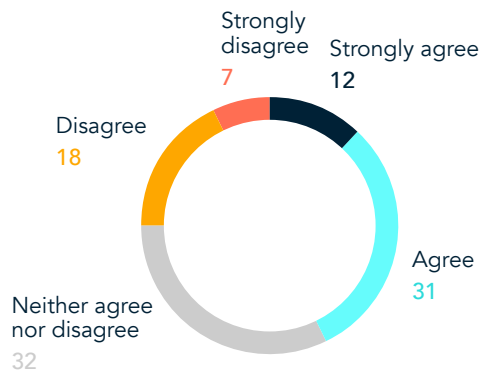


Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 240 information security professionals
 Note: Respondents could choose more than one answer.

In terms of growth opportunities, 43% either agree or strongly agree that they do have opportunities within their current company.

Executive beliefs about growth opportunities at their current company (%)

There are opportunities for me to further grow



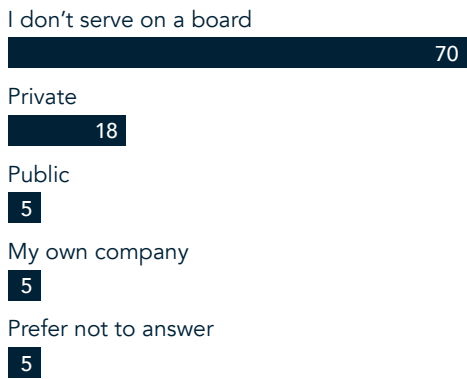
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 262 information security professionals

In 2023, the share of CISOs who sit on a corporate board more than doubled, from 14% in 2022 to 30% in 2023. And while nearly three-quarters of CISOs do not serve on a corporate board, the vast majority of those want to.



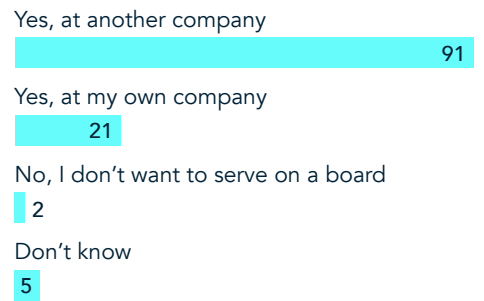
Board service (%)

Do you currently serve on a corporate board of your or any other company, public or private?



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 242 information security professionals

Would you like to serve on a corporate board at your or any other company, public or private?

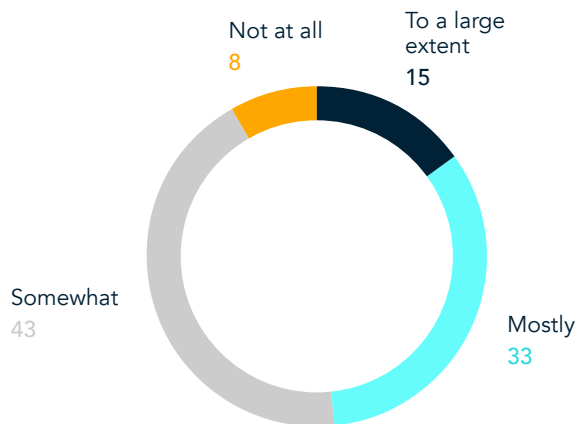


Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 168 information security professionals

And that's good news, because cybersecurity experience is sorely needed on boards: slightly less than half of CISOs say that the board has the knowledge or expertise to respond effectively to their presentations.

Attitudes around board exposure and effectiveness (%)

Board has knowledge or expertise to respond effectively to cyber presentations



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 243 information security professionals

Note: Numbers may not sum to 100%, because of rounding.

This lack of expertise is unsurprising, given the generally low incidence of board appointments going to people with cybersecurity experience. Our *Board Monitor US 2023* report, for example, shows that only 14% of seats were filled by those with cybersecurity expertise,⁶ while the figures were 3% and 5% in the United Kingdom⁷ and Europe,⁸ respectively.

That said, the topic of who is qualified to be a cyber expert on boards is complex. Companies can look to CIOs and CTOs as well as CISOs, and perhaps executives in risk or compliance. Regardless, this

expertise is more and more crucial on boards, and we are seeing that despite an increased focus and investment in cybersecurity, as evidenced by growing compensation and team size and evolving reporting relationships, that interest is still not resulting in board memberships for those experts. In light of the oncoming challenges inherent in such technologies as AI and machine learning, cyberattacks, and geopolitical risk, boards must arm themselves with the expertise to respond to these and other yet unknown threats.

⁶ *Board Monitor US 2023*,
Heidrick & Struggles, heidrick.com.

⁷ *Board Monitor UK 2023*,
Heidrick & Struggles, heidrick.com.

⁸ *Board Monitor Europe 2023*,
Heidrick & Struggles, heidrick.com.

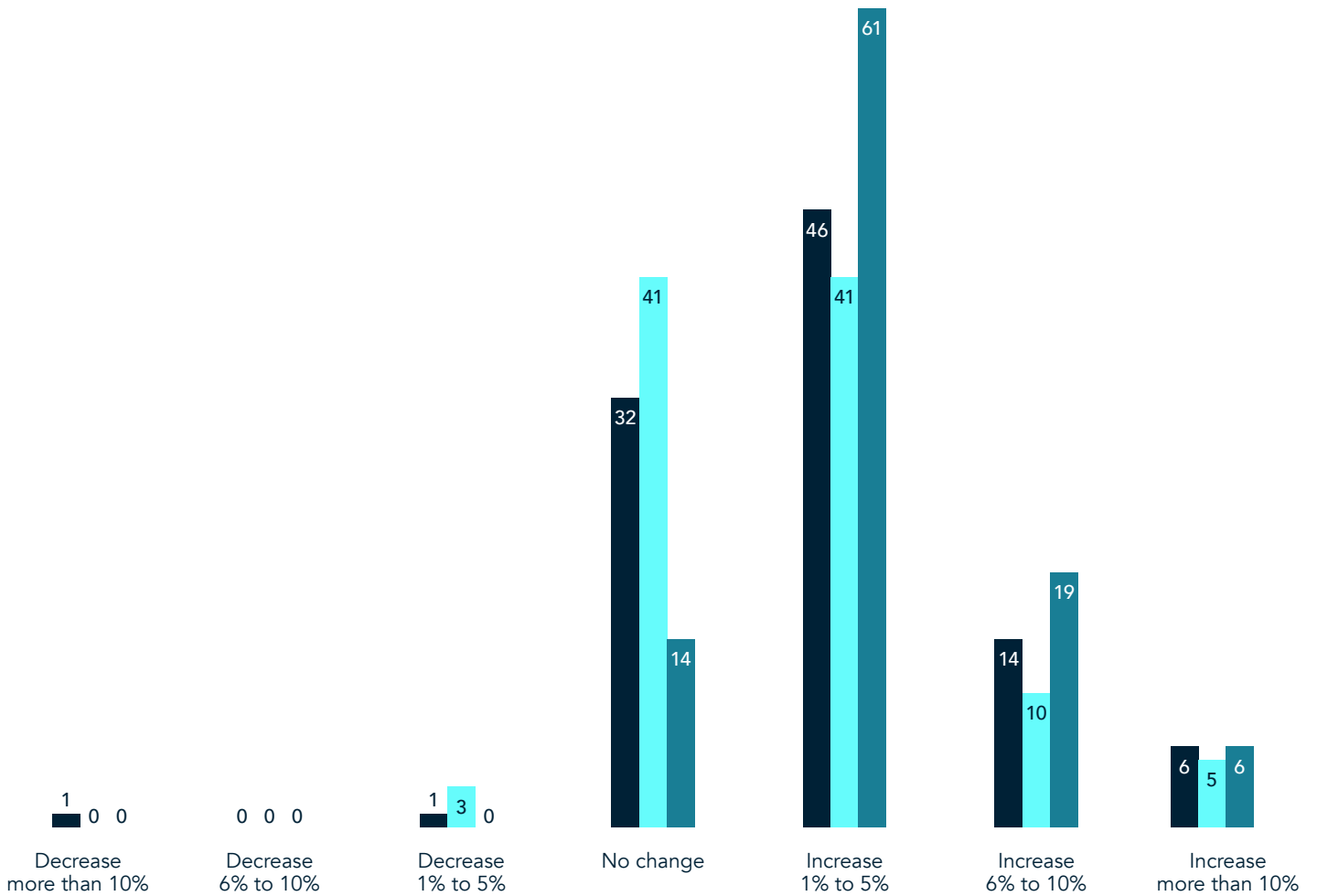
The state of CISO compensation

Across regions, respondents generally expect their cash base to either remain the same or increase modestly in the coming year.

Cash base expectations, by country (%)

■ United States ■ Europe ■ Australia

Year-over-year change in cash base compensation expectations



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 148 information security professionals in the United States; Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 39 information security professionals in Europe; and Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 36 information security professionals in Australia

CISO compensation: United States

For CISOs in the United States, compensation has generally continued to increase. Reported median total cash compensation increased 6% year over year, to \$620,000 in 2023, up from \$584,000 in 2022. Median total compensation, including any annualized equity grants or long-term incentives, also increased, to \$1,100,000 this year, up from \$971,000 last year.

Those in the financial services industry reported the highest average total compensation, \$1,734,000, while those at industrial companies reported the lowest. CISOs in the technology and services industry received the highest average annual equity/LTI. Compensation generally rises along with company revenue and team size.

Higher compensation did not, however, necessarily correlate with longer tenure. Those with tenure between one and two years saw higher compensation across base, bonus, and equity/LTI than did those with longer tenure, which is reflective of the robust talent market of 2022 and 2021, when new CISOs, those with less than one year of tenure, generally reported higher compensation than their peers with more years of experience.

As in last year's report, we see some variation in compensation across US regions. For cash compensation, CISOs in the Mid-Atlantic and Southwest reported the highest average, at \$915,000 and \$807,000, respectively. Last year, CISOs in the Northeast and Southwest reported the highest figure.

When annualized equity is added in, West Coast CISOs once again top the list, at \$2,131,000.

Last year for the first time we included the 95th percentile in order to understand the compensation range of the most highly valued talent. We anticipated that the cooling off of equity markets could impact the highest paid CISOs, which proved partly true: the 95th percentile decreased for those in technology and services, healthcare and life sciences, and consumer companies, but increased for those in financial services and industrial companies. There is still a very wide disparity between the "average CISO" and the highest paid.

As for reporting lines, those that report to the CEO saw the highest average total compensation. However, there were variations in highest average base, bonus, and annual equity/LTI.

Generally, those that serve on a board reported slightly higher compensation.

United States compensation trends

(USD, thousands)

	n	Base				Bonus				Total cash compensation				Annual equity/LTI				Total compensation			
		25th	avg.	75th	95th	25th	avg.	75th	95th	25th	avg.	75th	95th	25th	avg.	75th	95th	25th	avg.	75th	95th
Overall	149	330	451	500	900	120	308	370	1,100	480	759	935	1,800	200	724	900	3,000	765	1,483	1,785	3,800
Industry																					
Financial services or fintech	44	400	509	580	1,000	200	523	688	1,395	600	1,032	1,200	2,200	200	702	1,030	2,000	970	1,734	2,300	3,800
Industrial, manufacturing, energy	18	340	365	400	450	150	192	270	300	480	557	650	720	200	321	360	1,080	750	878	950	1,800
Technology and services	48	300	442	480	1,000	100	205	250	500	400	647	830	1,420	300	1,080	1,400	3,000	800	1,727	1,923	5,255
Healthcare, biotech, life sciences	15	380	413	450	540	100	214	200	550	550	627	700	1,000	250	379	500	600	858	1,006	1,243	1,540
Consumer, retail, media	19	300	493	550	1,400	140	289	300	1,400	440	782	850	2,800	130	633	900	3,000	620	1,415	1,700	4,200
Revenue																					
Less than \$1.00bn	20	255	348	443	576	60	135	150	550	370	483	550	920	80	499	645	1,900	560	982	1,220	2,530
\$1.00bn–\$4.99bn	30	350	492	520	1,200	100	233	300	580	530	725	920	1,400	213	1,030	1,500	3,000	920	1,755	2,080	3,850
\$5.00bn–\$9.99bn	23	320	410	450	550	140	228	300	440	450	638	700	1,000	200	649	600	3,000	760	1,287	1,500	3,500
\$10.00bn–\$19.99bn	25	340	481	500	750	170	323	430	600	530	804	970	1,200	200	462	600	1,250	780	1,266	1,600	2,250
\$20.00bn–\$49.99bn	24	330	460	503	900	130	438	500	1,300	470	898	990	1,800	250	737	1,075	2,000	730	1,635	2,600	3,800
More than \$50.00bn	24	390	498	550	800	200	435	550	1,100	650	933	1,100	1,800	250	776	1,080	1,700	950	1,709	2,150	3,300
Team size																					
0–25	33	280	402	408	1,320	70	173	180	300	370	575	610	1,420	110	307	500	660	560	882	1,050	1,720
26–50	32	300	386	400	800	100	213	248	550	430	599	665	1,100	170	378	400	900	700	977	1,158	1,840
51–100	26	350	498	500	1,100	123	268	293	1,000	523	766	838	1,400	200	728	1,013	3,000	750	1,494	1,500	3,300
More than 100	58	400	491	550	760	200	452	550	1,300	630	943	1,050	1,800	400	1,122	1,500	3,000	1,163	2,065	2,583	3,830
Tenure																					
Less than 1 year	24	308	405	445	530	143	230	300	550	465	635	775	1,030	200	545	400	1,030	640	1,180	1,340	1,910
1–2 years	46	350	459	520	800	103	374	508	1,200	530	833	1,000	1,800	250	822	1,275	2,570	930	1,655	2,400	3,650
3–4 years	38	330	422	450	750	108	254	298	810	463	676	753	1,430	200	705	600	3,000	768	1,381	1,315	3,800
5 or more years	40	300	500	530	1,400	115	306	358	1,400	423	806	998	2,800	200	761	1,000	3,000	750	1,567	2,050	3,830
US region																					
Northeast	38	320	445	500	1,200	100	339	460	1,200	433	784	1,038	1,800	150	454	500	1,500	780	1,238	1,500	3,300
Mid-Atlantic	12	328	500	663	1,100	170	415	550	1,100	520	915	1,100	2,200	200	534	600	2,000	730	1,449	1,700	3,800
Southeast	17	320	477	500	1,000	140	316	500	780	530	793	1,000	1,350	250	728	900	2,500	1,100	1,521	1,840	2,800
Midwest	29	330	415	420	750	140	223	290	440	480	638	793	1,050	200	577	545	2,600	660	1,215	1,530	3,520
Southwest	16	340	453	450	1,500	180	354	350	1,600	520	807	900	3,100	313	584	675	2,000	830	1,391	1,800	3,800
Mountain West	5	300	362	430	450	70	110	130	200	370	472	580	630	200	850	1,500	1,500	830	1,322	2,080	2,080
West Coast	30	330	472	530	900	100	319	388	1,400	465	791	830	1,800	500	1,340	2,100	4,100	868	2,131	3,250	5,330

Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 149 information security professionals

United States compensation trends: Median year-over-year comparison

(USD, thousands)

	n	Base		Bonus		Total cash compensation		Annual equity/LTI		Total compensation	
		2023	2022	2023	2022	2023	2022	2023	2022	2023	2022
Overall	149	400	376	200	195	620	584	400	326	1,100	971
Industry											
Financial services or fintech	44	450	451	400	330	980	847	500	276	1,500	1,132
Industrial, manufacturing, energy	18	355	326	190	133	535	441	250	188	830	634
Technology and services	48	400	376	150	165	560	547	600	651	1,250	1,296
Healthcare, biotech, life sciences	15	430	376	200	148	620	546	400	351	1,035	922
Consumer, retail, media	19	380	376	205	250	585	656	375	326	1,050	976
Revenue											
Less than \$1.00bn	20	330	376	100	115	460	472	400	451	1,040	1,171
\$1.00bn–\$4.99bn	30	400	376	200	171	650	546	500	276	1,330	951
\$5.00bn–\$9.99bn	23	400	326	195	144	600	474	300	150	1,000	699
\$10.00bn–\$19.99bn	25	400	376	250	208	680	696	320	326	1,000	1,026
\$20.00bn–\$49.99bn	24	400	451	200	306	580	757	450	326	985	1,082
More than \$50.00bn	24	450	451	330	292	940	701	550	451	1,540	1,326
Team size											
0–25	33	325	326	100	115	445	409	200	150	700	659
26–50	32	370	376	185	153	545	509	300	276	910	931
51–100	26	410	376	190	195	600	584	355	326	1,080	976
More than 100	58	450	451	360	306	900	778	725	451	1,700	1,335
Tenure											
Less than 1 year	24	385	451	200	208	600	655	305	326	970	1,079
1–2 years	46	410	376	205	207	650	584	565	376	1,300	959
3–4 years	38	380	376	200	151	565	558	380	276	945	974
5 or more years	40	400	376	200	171	650	547	450	226	1,200	883
US region											
Northeast	38	400	376	210	215	660	612	300	326	1,050	959
Mid-Atlantic	12	400	376	270	148	650	509	255	150	910	739
Southeast	17	500	351	290	171	825	565	700	226	1,340	801
Midwest	29	360	376	200	191	560	565	280	276	915	881
Southwest	16	400	326	220	221	700	612	400	276	1,100	856
Mountain West	5	380	413	90	156	470	541	850	150	1,455	669
West Coast	30	425	413	170	183	610	584	830	951	1,630	1,652

Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 149 information security professionals

United States compensation trends

(USD, thousands)

	n	Base				Bonus				Total cash compensation				Annual equity/LTI				Total compensation			
		25th	avg.	75th	95th	25th	avg.	75th	95th	25th	avg.	75th	95th	25th	avg.	75th	95th	25th	avg.	75th	95th
Reports to:																					
CEO	5	300	480	520	1,000	63	275	513	550	295	755	920	920	500	1,575	2,575	2,600	1,200	2,330	3,520	3,520
CIO	53	330	453	500	1,000	140	350	400	1,200	470	803	970	1,800	200	531	583	2,000	660	1,334	1,530	3,800
CTO/senior engineering exec	26	370	457	450	750	100	213	210	350	500	670	670	1,050	213	1,122	1,975	3,000	870	1,792	2,500	3,830
COO or CAO	19	340	467	580	750	200	354	500	810	520	821	1,000	1,430	170	944	1,000	4,500	830	1,765	2,200	5,530
Global CISO	12	270	459	430	1,320	70	232	140	1,400	390	691	940	1,800	225	468	575	1,400	790	1,159	1,720	2,300
Chief risk officer or senior regulatory executive	10	280	448	500	1,100	150	376	460	1,100	430	824	990	2,200	100	322	400	1,100	600	1,146	1,490	3,300
CFO	9	350	409	500	550	150	286	380	550	480	695	880	1,100	300	564	700	1,100	780	1,259	1,700	2,200
Other	11	300	447	540	900	130	299	400	500	525	746	930	950	300	811	1,000	3,000	863	1,557	2,213	3,500
Serves on board																					
No	113	320	452	495	1,000	120	297	330	1,000	480	749	920	1,440	250	706	800	2,600	783	1,455	1,698	3,800
Yes	36	330	448	540	600	120	339	400	1,200	460	787	970	1,800	160	784	1,030	3,000	648	1,571	2,300	3,850

Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 149 information security professionals

Base compensation increased across almost every industry, while there was more variation in bonus as a percent of total compensation; CISOs in consumer, retail, and media companies saw an 18% year-over-year drop. As opposed

to last year, annual equity generally increased across industries, with the exception of technology and services.

Bonuses notably dropped year over year for those at companies with a revenue

of \$20.00 billion to \$49.99 billion, and total compensation dropped for those with a tenure of less than a year—the latter likely being a reflection of a significantly cooled talent market.

United States compensation trends: Median year-over-year change (%)

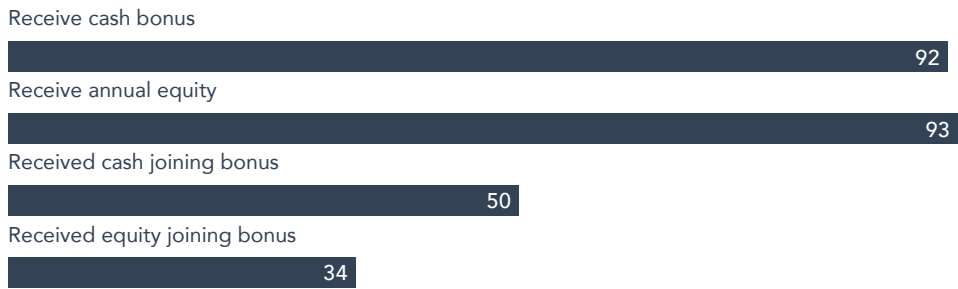
	Base	Bonus	Total cash compensation	Annual equity/LTI	Total compensation
Overall	7%	2%	6%	23%	13%
Industry					
Financial services or fintech	0%	21%	16%	81%	33%
Industrial, manufacturing, energy	9%	43%	21%	33%	31%
Technology and services	7%	-9%	2%	-8%	-4%
Healthcare, biotech, life sciences	15%	35%	13%	14%	12%
Consumer, retail, media	1%	-18%	-11%	15%	8%
Revenue					
Less than \$1.00bn	-12%	-13%	-3%	-11%	-11%
\$1.00bn-\$4.99bn	7%	17%	19%	81%	40%
\$5.00bn-\$9.99bn	23%	35%	27%	100%	43%
\$10.00bn-\$19.99bn	7%	20%	-2%	-2%	-3%
\$20.00bn-\$49.99bn	-11%	-35%	-23%	38%	-9%
More than \$50.00bn	0%	13%	34%	22%	16%
Team size					
0-25	0%	-13%	9%	33%	6%
26-50	-1%	21%	7%	9%	-2%
51-100	9%	-3%	3%	9%	11%
More than 100	0%	18%	16%	61%	27%
Tenure					
Less than a year	-15%	-4%	-8%	-6%	-10%
1-2 years	9%	-1%	11%	50%	36%
3-4 years	1%	33%	1%	38%	-3%
5 or more years	7%	17%	19%	100%	36%

In terms of bonuses, while the vast majority of respondents received bonuses and annual equity, only half reported receiving a cash joining bonus

and about one-third reported receiving an equity joining bonus. Those in financial services reported the highest average cash bonus, while those in

technology and services reported the highest average equity bonus.

Share of respondents that say they... (%)



United States: Joining or sign-on bonus

(USD, thousands)

	n	Cash				Total compensation			
		25th	avg.	75th	95th	25th	avg.	75th	95th
Overall	149	1,100	1,431	1,400	1,900	1,200	2,007	2,000	5,500
Industry									
Financial services or fintech	44	1,150	1,917	1,700	7,000	1,150	1,875	1,600	6,000
Industrial, manufacturing, energy	18	1,100	1,150	1,200	1,300	1,100	1,253	1,450	1,500
Technology and services	48	1,100	1,387	1,300	1,900	1,380	2,469	3,500	7,000
Healthcare, biotech, life sciences	15	1,100	1,201	1,300	1,500	1,313	2,231	3,513	3,950
Consumer, retail, media	19	1,100	1,247	1,400	1,600	1,100	1,626	2,000	2,800
Revenue									
Less than \$1.00bn	20	1,050	1,135	1,150	1,500	1,150	2,059	3,950	3,950
\$1.00bn–\$4.99bn	30	1,100	1,227	1,300	1,800	1,200	2,148	1,800	7,000
\$5.00bn–\$9.99bn	23	1,100	1,264	1,405	1,700	1,300	2,133	1,750	5,500
\$10.00bn–\$19.99bn	25	1,100	1,167	1,200	1,400	1,130	1,276	1,450	1,500
\$20.00bn–\$49.99bn	24	1,200	1,850	1,500	6,000	1,230	2,361	3,500	6,000
More than \$50.00bn	24	1,250	2,069	1,700	7,000	1,200	2,051	2,200	4,250
Team size									
0–25	33	1,050	1,131	1,150	1,500	1,060	1,671	1,500	3,950
26–50	32	1,100	1,210	1,300	1,500	1,188	1,498	1,788	1,900
51–100	26	1,100	1,568	1,250	7,000	1,200	1,416	1,380	2,800
More than 100	58	1,200	1,656	1,675	4,700	1,300	2,725	4,063	6,950
Tenure									
Less than 1 year	24	1,100	1,267	1,300	1,700	1,100	1,358	1,500	1,900
1–2 years	46	1,100	1,637	1,500	6,000	1,250	2,471	3,950	6,000
3–4 years	38	1,100	1,398	1,300	1,900	1,200	1,829	2,000	4,250
5 or more years	40	1,100	1,203	1,300	1,400	1,200	2,933	5,500	7,000
US region									
Northeast	38	1,100	1,512	1,300	6,000	1,200	2,021	1,800	6,000
Mid-Atlantic	12	1,100	1,825	1,500	7,000	1,250	1,550	1,900	2,000
Southeast	17	1,158	1,348	1,650	1,700	1,263	1,913	3,025	3,500
Midwest	29	1,100	1,260	1,400	1,800	1,150	1,686	1,750	5,000
Southwest	16	1,100	1,250	1,450	1,600	1,225	1,295	1,360	1,380
Mountain West	5	1,030	1,077	1,100	1,100	1,060	1,130	1,200	1,200
West Coast	30	1,113	1,471	1,400	4,700	1,463	3,059	4,175	7,000

CISO compensation: Europe

The average total cash compensation for CISOs in Europe was \$457,000. Average total compensation, including any annualized equity grants or long-term incentives, was \$552,000. As in the United States and Australia, those in the financial services industry reported the highest average total cash compensation, at \$623,000.

However, in Europe, those at healthcare and life sciences companies reported the lowest. Average annual equity/LTI was highest for those in technology and services.

Across regions, as expected, compensation generally rises along with company revenue and team size.

Europe compensation trends

(USD, thousands)

	n	Base				Bonus				Total cash compensation				Annual equity/LTI				Total compensation			
		25th	avg.	75th	95th	25th	avg.	75th	95th	25th	avg.	75th	95th	25th	avg.	75th	95th	25th	avg.	75th	95th
Overall	38	180	301	320	950	43	156	150	550	230	457	528	1,450	33	95	173	200	273	552	600	929
Industry																					
Financial services or fintech	17	220	422	500	990	70	201	230	550	300	623	700	1,540	50	126	200	280	360	749	800	900
Industrial, manufacturing, energy	7	120	174	200	300	20	210	100	1,030	140	384	400	1,180	10	28	53	60	140	412	460	460
Technology and services	4	200	290	415	450	70	148	248	280	270	438	663	730	48	128	195	200	318	566	858	930
Healthcare, biotech, life sciences	2	150	180	210	210	30	35	40	40	180	215	250	250	20	30	40	40	220	245	270	270
Consumer, retail, media	6	180	218	300	300	30	68	90	150	230	286	270	450	38	110	188	200	260	396	600	600
Revenue																					
\$4.99bn or less	18	150	292	360	950	30	141	100	1,030	180	433	410	1,180	50	111	200	280	300	544	715	900
\$5.00bn or more	18	180	314	310	990	50	165	150	550	230	479	460	1,540	23	92	173	200	260	571	600	930
Team size																					
50 or fewer	23	150	272	320	900	30	163	120	1,030	200	435	350	1,450	30	57	60	140	260	492	400	600
More than 50	15	210	345	400	990	70	147	150	550	300	492	600	1,540	50	141	200	280	460	633	800	930
Tenure																					
2 or fewer years	18	190	311	360	950	50	180	150	1,030	250	491	550	1,180	40	90	150	200	283	581	600	900
3 or more years	20	173	292	308	986	40	138	150	550	220	430	460	1,540	30	99	180	280	230	529	595	930

CISO compensation: Australia

The average total cash compensation for CISOs in Australia was \$368,000. Average total compensation, including any annualized equity grants or long-term incentives, was \$586,000. As in the United States and Europe, those in the financial services industry

reported the highest average total cash compensation, at \$501,000.

As expected, compensation generally rises along with company revenue and team size.

Australia compensation trends

(USD, thousands)

	n	Base				Bonus				Total cash compensation				Annual equity/LTI				Total compensation			
		25th	avg.	75th	95th	25th	avg.	75th	95th	25th	avg.	75th	95th	25th	avg.	75th	95th	25th	avg.	75th	95th
Overall	37	200	266	300	430	33	102	128	300	240	368	450	650	50	218	250	1,000	410	586	780	2,000
Industry																					
Financial services or fintech	11	280	351	420	600	50	150	250	400	340	501	520	1,000	90	227	170	1,000	410	728	800	2,000
Industrial, manufacturing, energy	6	210	230	260	260	30	77	100	120	270	307	350	360	30	30	30	30	270	337	390	390
Technology and services	11	200	227	300	350	20	106	200	270	220	333	500	620	75	276	363	1,000	490	609	850	1,620
Other	9	200	253	320	360	13	51	85	130	213	304	418	450	10	163	330	330	220	467	780	780
Revenue																					
Less than \$1.00bn	11	180	227	300	350	25	104	188	270	223	331	488	620	50	280	400	1,000	570	611	850	1,620
\$1.00bn–\$4.99bn	11	210	274	300	430	20	50	90	100	240	324	350	520	30	93	150	170	270	417	670	690
\$5 billion or more	10	213	311	380	600	70	159	250	400	245	470	600	1,000	30	277	330	1,000	410	747	800	2,000
Team size																					
50 or fewer	25	200	247	290	350	20	85	100	270	230	332	360	620	35	258	238	1,000	390	590	700	2,000
More than 50	12	220	314	400	430	90	140	200	300	388	454	520	650	50	171	300	400	410	625	800	850
Tenure																					
2 or fewer years	16	203	273	300	600	30	98	100	400	230	371	410	1,000	150	475	1,000	1,000	543	846	1,905	2,000
3–4 years	11	180	227	280	400	30	103	120	250	240	330	380	650	10	66	150	200	270	396	700	800
5 or more years	10	260	308	398	430	50	106	130	300	310	414	503	520	100	166	170	330	430	580	690	780

Specialty Practices

Heidrick & Struggles' Specialty Practices provide expertise on emerging technologies.

These practices include:

- Artificial Intelligence, Data, and Analytics
- Blockchain/Distributed Ledger Technology
- Cybersecurity
- Digital Innovation
- Internet of Things

Leader of Heidrick & Struggles' Specialty Practices

Global

Sam Burman
Global Managing Partner
sburman@heidrick.com

Technology Officers Practice

The world is currently experiencing a revolution. With technology constantly advancing, the contemporary business landscape is now defined by rapid innovation. Advances in cloud computing, artificial intelligence, machine learning, and the Internet of Things have enabled companies to become lean, agile, and efficient competitors in the global market. Indeed, the promise of a digital future has convinced organizations across all industry segments to adopt more technology-focused business strategies.

At Heidrick & Struggles, we believe that leadership plays an essential role in this transformation. That is why our Technology Officers Practice is committed to helping our clients find the next-generation technology talent necessary to take their organizations to the next level. Our executive search consultants bring unparalleled experience, having successfully placed more than 1,000 information and technology functional officers with some of the best-known and most-admired companies around the world.

Leader of Heidrick & Struggles' Technology Officers Practice

Global

Katie Graham Shannon
Managing Partner
kshannon@heidrick.com