2024 Global Chief Information Security Officer Organization and Compensation Survey

Contents

A message from the authors

Welcome to our *2024 Global Chief Information Security Officer Organization and Compensation Survey*, our fifth annual examination of 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 summer 2024 of 416 CISOs around the world. Most carried the title of chief information security officer, but respondents also included chief security officers and other senior information security executives. This report includes organizational and compensation data from respondents in the United States, Europe, Asia Pacific, and the Middle East.

We hope you enjoy reading the report, which is now widely recognized as the most authoritative and broadly 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,

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 compensation data, 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.

Matt Aiello
Partner
San Francisco
maiello@heidrick.com

Marie McGinnis
Principal
San Francisco
mmcginnis@heidrick.com

Max Randria
Partner
Melbourne
mrandria@heidrick.com

Guy Shaul
Partner
London
gshaul@heidrick.com

Scott Thompson
Partner
New York
sthompson@heidrick.com

Karthik Vedagiri
Partner
Bangalore
kvedagiri@heidrick.com

On confidentiality

The global chief information security officer (CISO) survey, 2024, 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

This year's survey of chief information security officers (CISOs) shows a maturing function with a wide range of risks upon which to focus. More of these leaders now report directly to the CEO or outside of the technology function (such as the CIO or CTO), signaling this role's movement closer to the center of the business and a shift to more enterprise risk responsibilities. Across all industries, respondents cited similar, ongoing threats to organizational cybersecurity as they did in last year, including advancements in artificial intelligence and machine learning and cyberattacks, which include nation-state attacks.

Slightly less than half of respondents do not have an internal successor in place in the event the CISO leaves unexpectedly. This can be quite costly given the competitiveness in the market for top cybersecurity talent and the premium companies pay for top talent.

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.

Key findings

Organizational structure and risks

- In terms of reporting structure, 14% of respondents report directly to the CEO, up from 5% in 2023. By region, a notable 35% of respondents from Hong Kong and Singapore report to the CEO, while only 9% of US respondents say the same.
- Overall, there was decrease in the share of respondents who report to the top technology executive (such as the CIO or CTO): from 54% in 2023 to 48% in 2024.
- Of those who do report to the CEO, US respondents most often said they are a member of the executive leadership team at their company.
- Sixty-three percent of respondents said they have been in their role for at least three years. This is notably higher than last year's survey, in which just over half of respondents said the same. We believe that this reflects improved performance in the role.
- We asked again this year about the risks, both personal and professional, that CISOs face in their role. Unsurprisingly, the most often cited cybersecurity risk was ransomware, followed by geopolitical risks, such as nation-state actors, and then AI.
  - By region, respondents in the United Kingdom most often cited ransomware as a top threat, and least often cited nation-state actors.
  - Respondents in India least often cited ransomware as a top threat, and most often cited AI.
- Looking to the future, respondents most often chose AI, machine learning, data analytics and product and application security as the most important areas to build or maintain expertise in over the next five years.
- Looking ahead, just over half, 53%, of respondents agreed that they have an internal successor in place who is just as good as or better than the external market can present.

Compensation

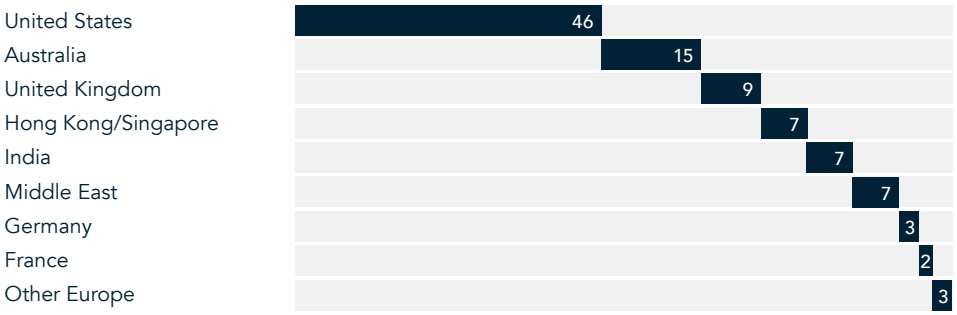
- US average total compensation, including cash base, bonus, and equity, was reported to be $1,648,000 in 2023.
- Average 2023 total compensation for respondents in Europe, including the United Kingdom, was $595,000.
- Average 2023 total compensation for respondents in Australia was $414,000.
- In Australia, Europe, and the United States, respondents at financial services firms generally reported the highest average compensation. While compensation data is not available this year for those respondents in Hong Kong and Singapore, India, and the Middle East, we hope to include those regions in future reports.

A look at this year's respondent profiles

Location

Respondents came from regions around the world.

Respondents' location (%)



Note: Numbers may not total 100% due to rounding.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 416

Company information

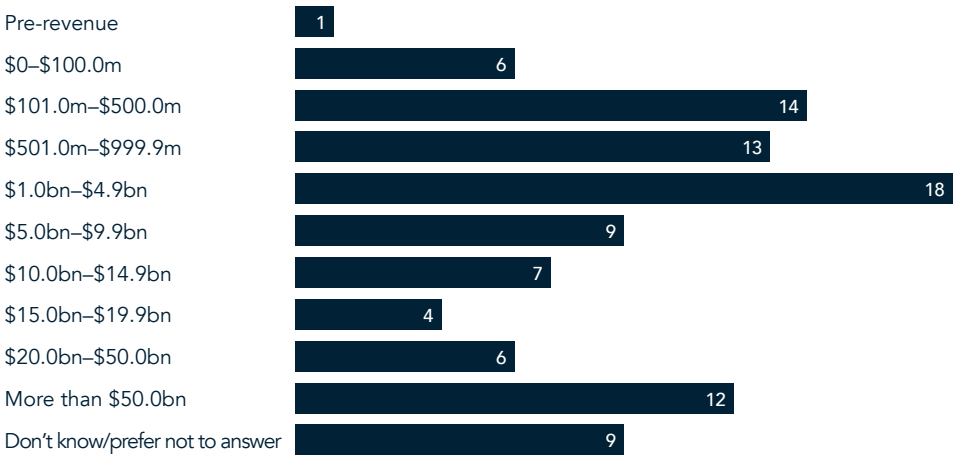
Slightly less than half of the CISOs were at companies with annual revenue of more than $5 billion, and they worked across a range of industries, most often technology and services and financial services.

Nearly half of respondents were at public companies.

Company ownership structure (%)

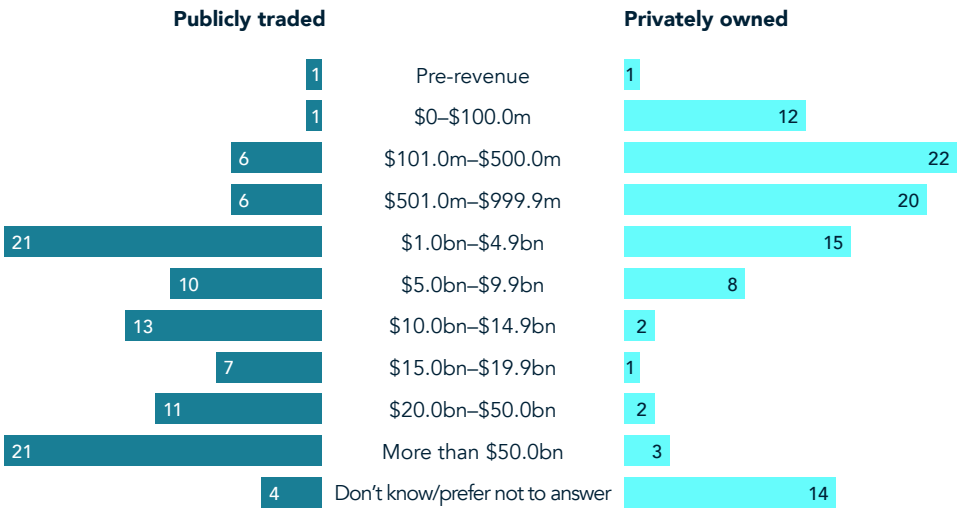
Note: Numbers may not total 100% due to rounding.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 354

Most recent annual revenue (USD) (%)



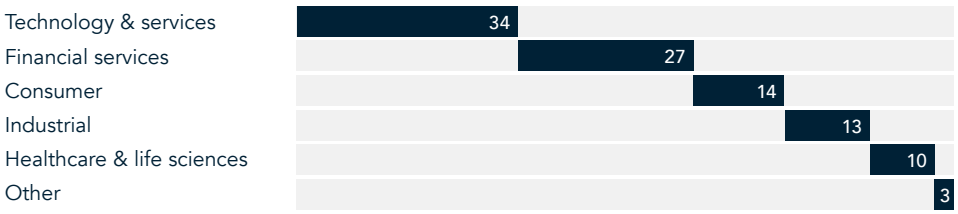
Note: Numbers may not total 100% due to rounding.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 354

Annual revenue, by company ownership (USD) (%)



Note: Numbers may not total 100% due to rounding.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 354

Current company industry (%)



Note: Numbers may not total 100% due to rounding.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 416

Role information

Sixty percent of respondents were chief information security officers.

Current role title (%)

Note: Respondents could choose more than one response.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 416

Similar to what we saw last year, average tenure was four years.

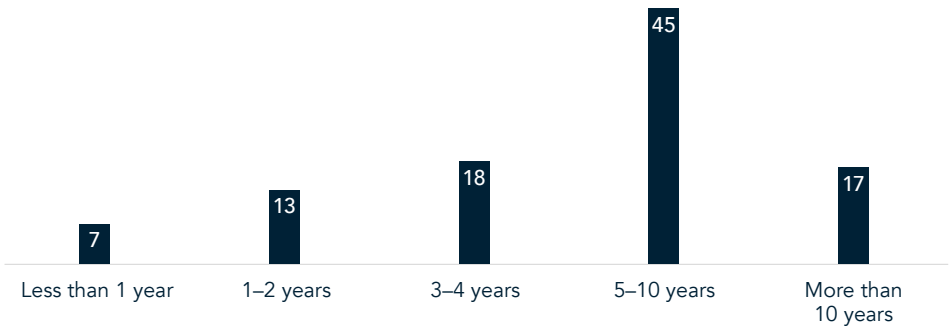
This year, 63% of respondents said they have been in their role for at least three years. This is notably higher than the share in last year's survey, in which just over half of respondents had been in their role for at least three years, and closer to the 77% who said the same in 2022.

Almost 20% of respondents said that their role has existed at their company for more than 10 years.

Tenure in current role (%)

Note: Numbers may not total 100% due to rounding.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 396

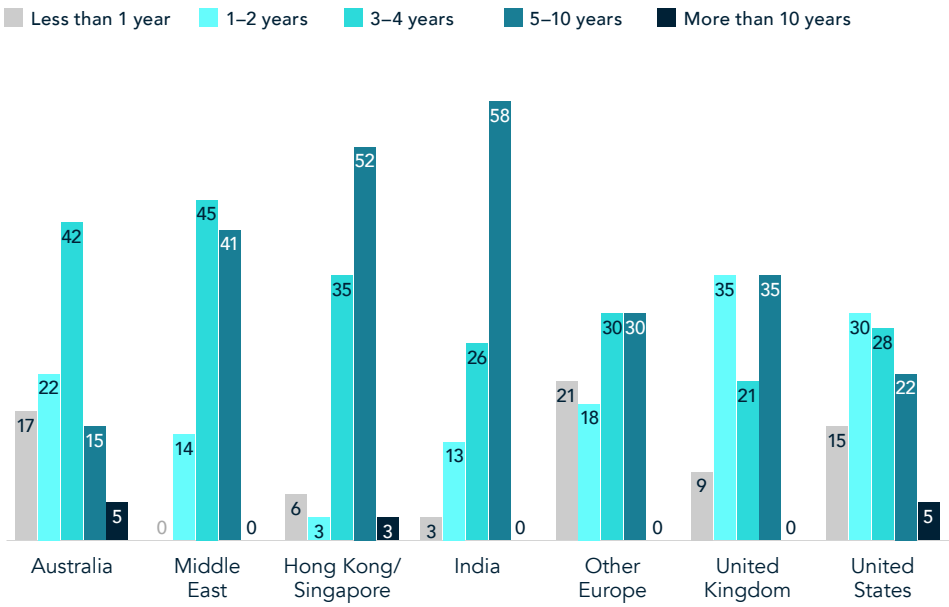
Years role has existed at the company (%)



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 393

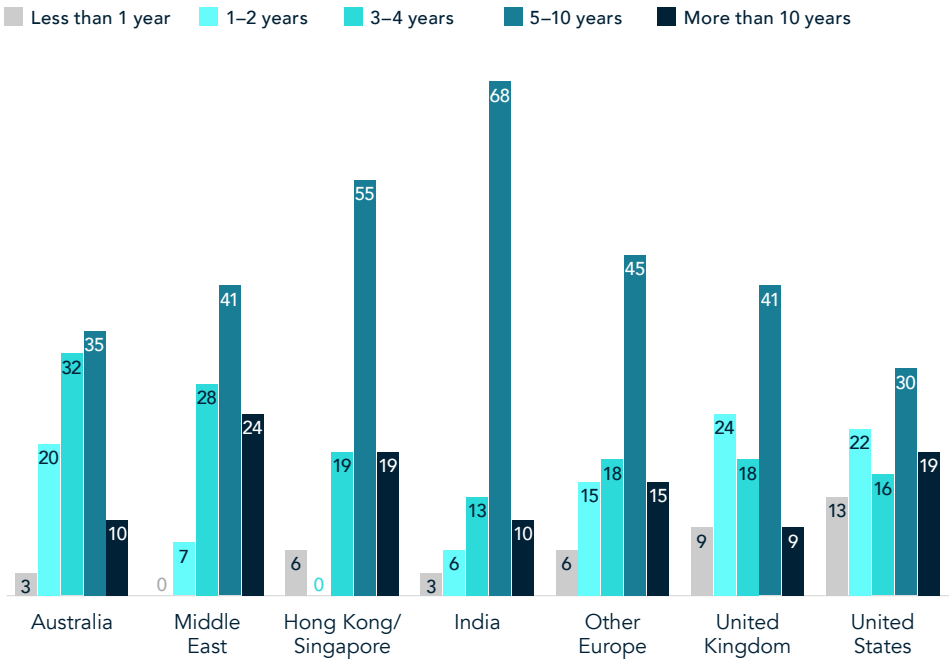
Looking across regions, respondents from Hong Kong and Singapore, India, and the Middle East most often reported the longest tenures in their current role, as well as the longest time their role has existed at their current company.

Tenure in current role, by region (%)



Note: Numbers may not total 100% due to rounding.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 396

Years role has existed at the company, by region (%)

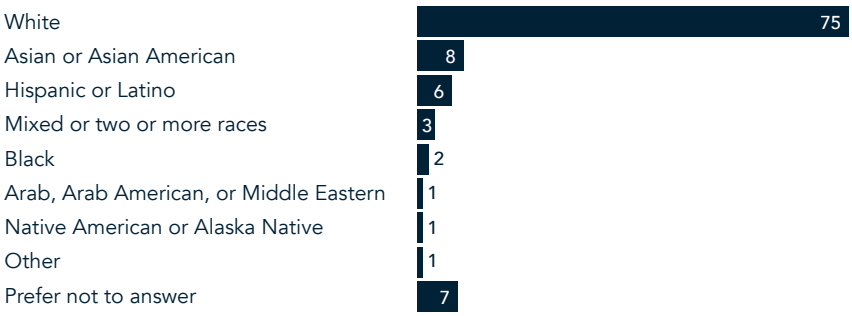


Note: Numbers may not total 100% due to rounding.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 393

Diversity and diversity initiatives

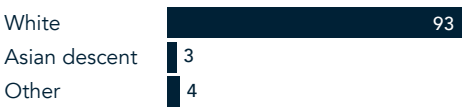
Globally, most respondents were male and white. In the United States, the share of non-white respondents fell to 20%, down from 32% in 2023 and closer to 2022's share of 22%. In the United Kingdom, only 7% of respondents were non-white. This low share warrants further exploration.

Race or ethnicity, United States (%)



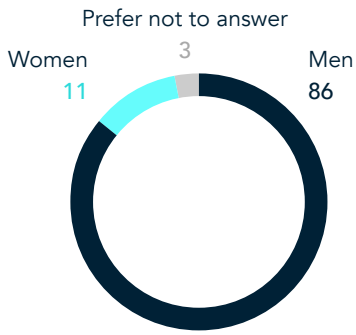
Note: Respondents could select more than one response.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 145

Race or ethnicity, United Kingdom (%)



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 29

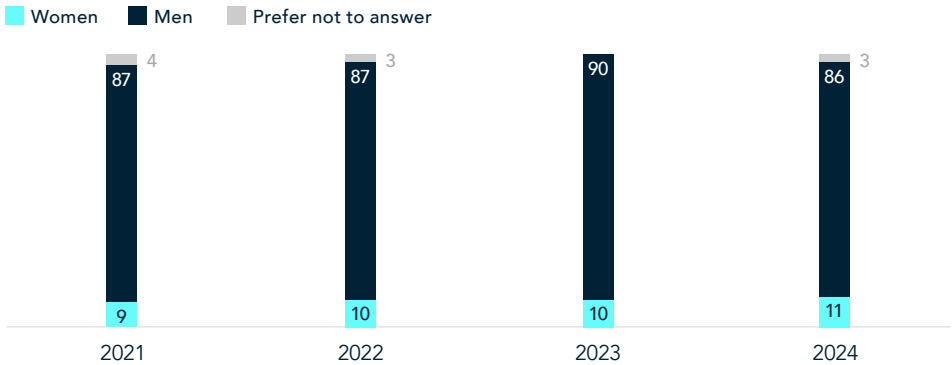
Gender (%)



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 353

Looking at the gender trends of all respondents to our annual surveys since 2021, the share of women in information security leaders roles is rising, though slowly.

Gender trends, 2021–2024 (%)

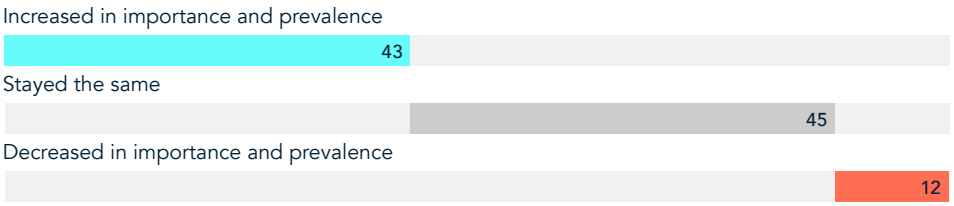


Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 353; Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 229; Heidrick & Struggles' global chief information security officer (CISO) survey, 2022, n = 327; Heidrick & Struggles' global chief information security officer (CISO) survey, 2021, n = 354

Across the world, respondents said that diversity initiatives have either stayed the same or increased in importance across their company as a whole.

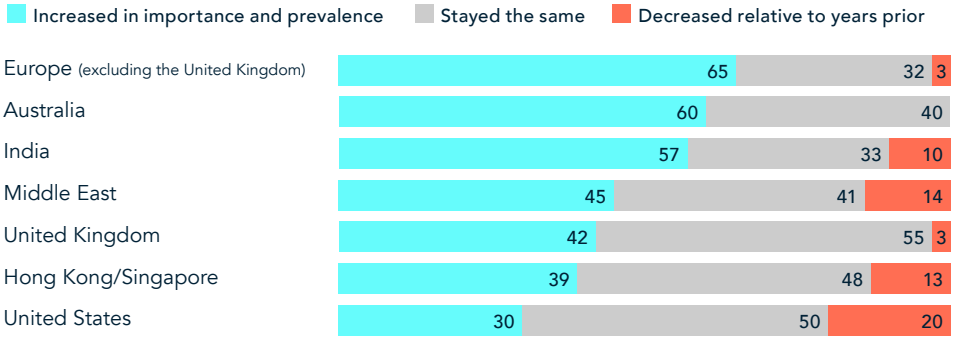
These initiatives have most often increased in importance in Europe (not including the United Kingdom), Australia, and India; they have most often decreased relative to years prior in the United States.

Importance of diversity initiatives this year compared to years prior (%)



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 369

Importance of diversity initiatives this year compared to years prior, by region (%)



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 369

What CISOs do all day: Reporting lines and remit

Nearly three-quarters of respondents said their function is directly included in the organization's business strategy.

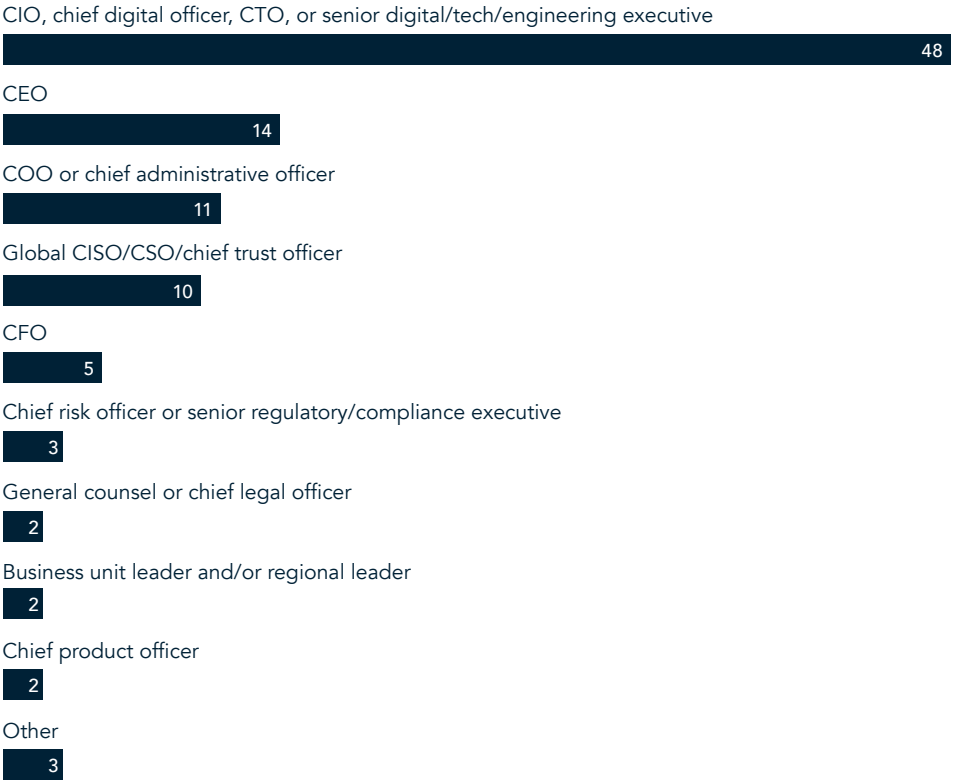
Is your function directly included in your organization's business strategy? (%)

Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 370

In terms of their own reporting structure, 14% report directly to the CEO, up from 5% in 2023. By region, a notable 35% of respondents from Hong Kong and Singapore report to the CEO, while only 9% of US respondents said the same.

However, US respondents who report to the CEO most often said that they are on the executive leadership team (see chart, "Are you a member of your company's executive leadership team?, by region." on page 14.)

To whom respondents report (%)



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 408

To whom respondents report, by region (%)

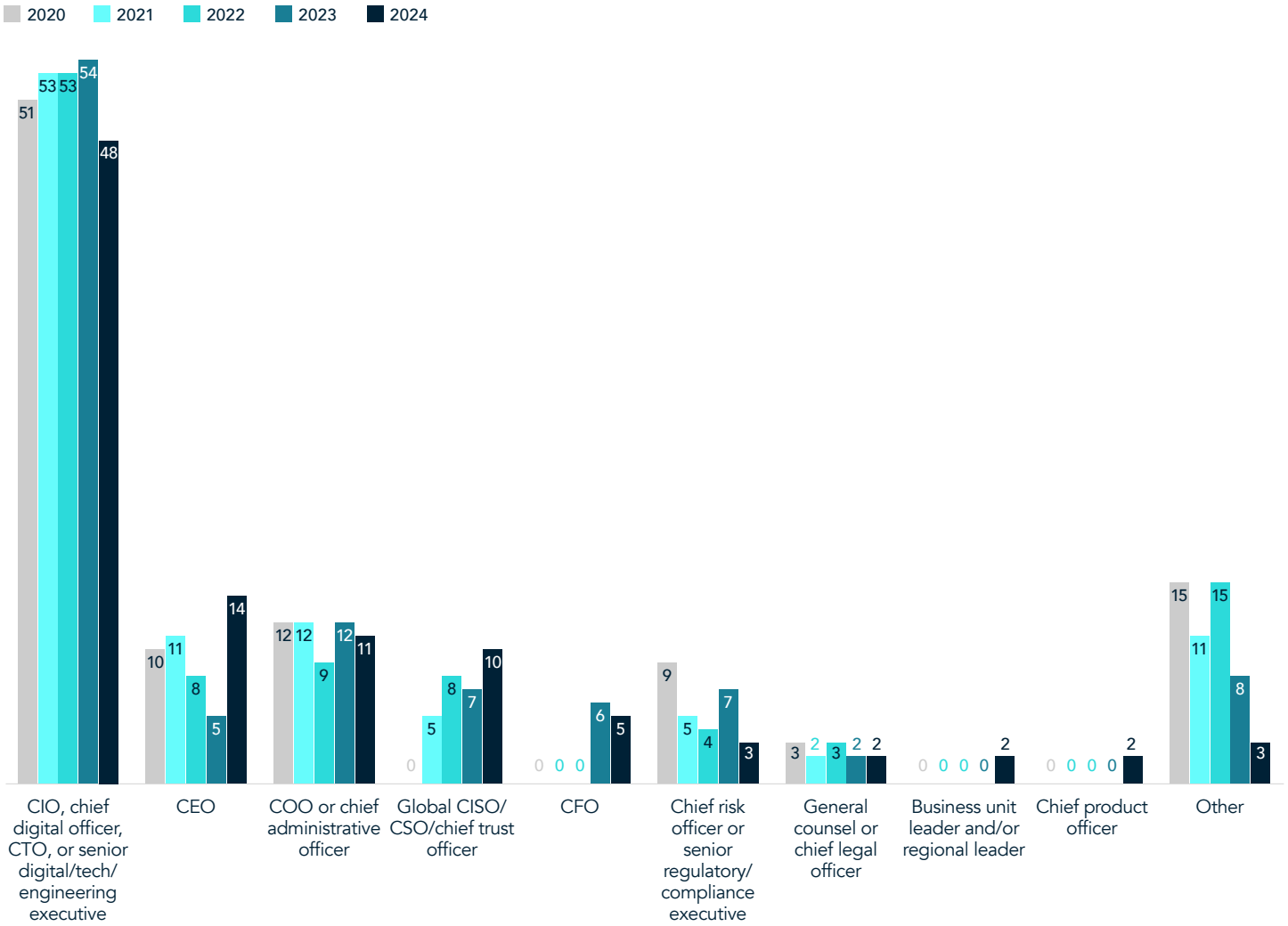
	Australia	Middle East	Hong Kong/ Singapore	India	Other Europe	United Kingdom	United States
CIO, chief digital officer, CTO, or senior digital/tech/engineering executive	70	28	29	45	43	44	49
CEO	2	24	35	29	20	14	9
COO or chief administrative officer	8	31	19	16	3	11	8
Global CISO/CSO/chief trust officer	2	10	0	3	17	8	15
CFO	5	0	16	3	6	3	5
Chief risk officer or senior regulatory/compliance executive	3	3	0	0	3	14	3
General counsel or chief legal officer	2	3	0	0	0	0	4
Business unit leader and/or regional leader	0	0	0	3	0	3	3
Chief product officer	2	0	0	0	3	3	2
Other	7	0	0	0	6	0	3

Note: Numbers may not total 100% due to rounding.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 408

Overall, there was decrease in those who report to the CIO, chief digital officer, CTO, or senior digital/tech/engineering executive—from 54% in 2023 to 48% in 2024.

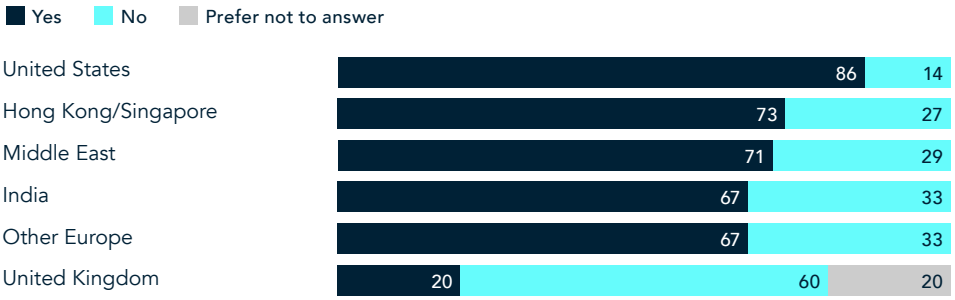
As we have noted in prior years' reports, we believe that the number of CISOs reporting to the technology function will continue to decrease as the CISO role takes a broader enterprise risk oversight role with direct ties to the audit committee and board.

To whom respondents report, year-over-year comparison (%)



Note: Numbers may not total 100% due to rounding.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 408; Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 243; Heidrick & Struggles' global chief information security officer (CISO) survey, 2022, n = 327; Heidrick & Struggles' global chief information security officer (CISO) survey, 2021, n = 354; Heidrick & Struggles' global chief information security officer (CISO) survey, 2020, n = 372

Are you a member of your company's executive leadership team?, by region (%)
(For those who report to the CEO)



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 52

As for where they spend the most time, respondents overall reported that they spend the most time working with network, cloud, and infrastructure; software development and product development and engineering; and legal, compliance, and risk. We expect that as the use of AI tools grows, information security officers will only spend more time with their colleagues in the legal function in order to ensure good governance of emerging AI tools.

It is also notable that though only 10% of respondents said that the board is among those with whom they spend the most time working, nearly half, 48%, said that they consult with the board.

Functions with whom CISOs and their teams spend the most time working and consulting (%)

	Spend the most time working with	Spend the most time consulting with	Overall
Network, cloud, infrastructure	56	30	86
Software development/product development/product engineering	43	39	82
Legal/compliance/risk	33	46	80
Corporate IT applications	25	53	78
Finance	10	57	67
Operations	23	41	64
Human resources	4	58	62
Corporate board of directors	10	48	58
Strategy	12	44	56
Business unit/P&L leaders	10	42	52
Marketing and customer engagement	5	43	48
Sales/go-to-market	6	36	43
Other	1	1	3

Note: Numbers may not sum to totals due to rounding.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 339

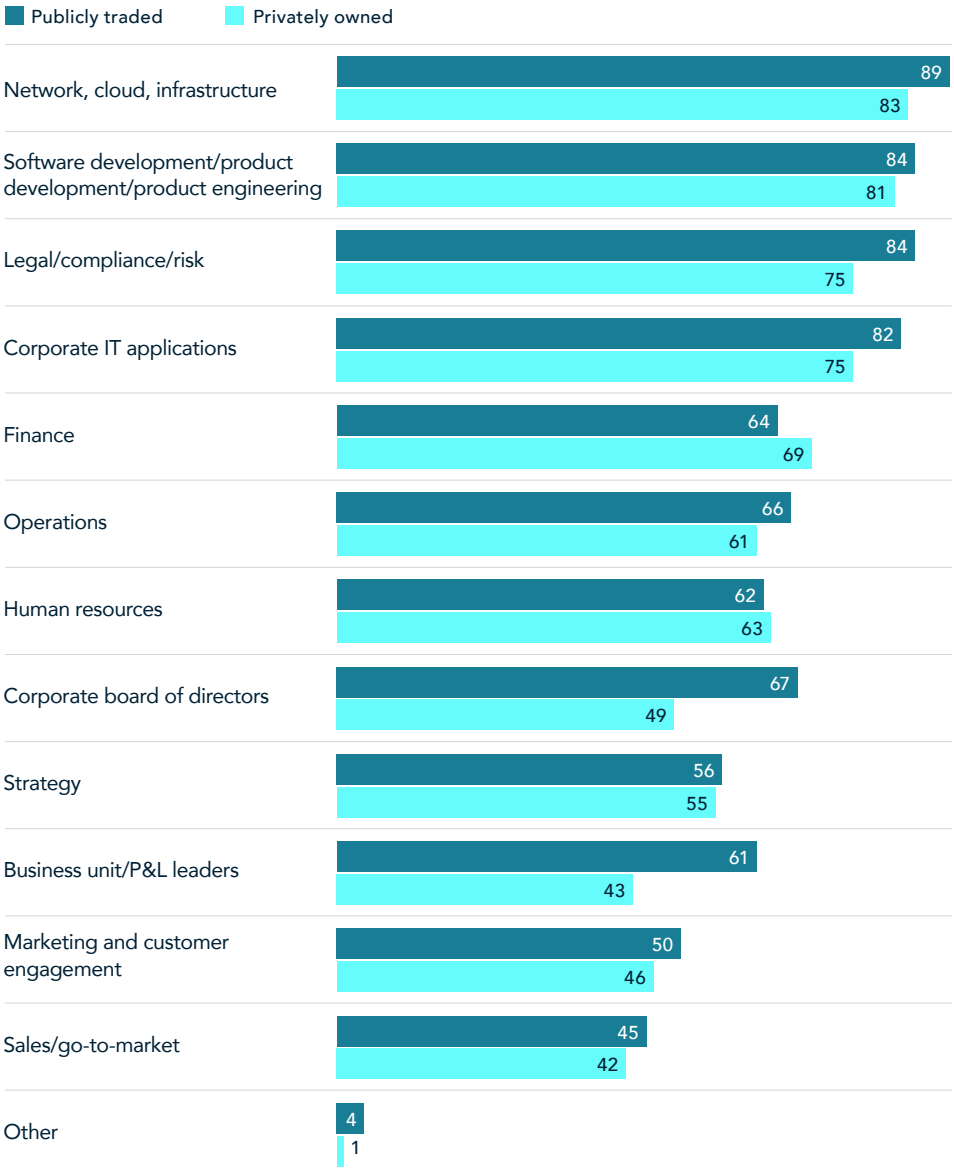
By region, respondents in Hong Kong and Singapore, India, and the Middle East least often named the board as one of their touchpoints.

Functions with whom CISOs and their teams have any touchpoints, by region (%)

Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 339

Overall, CISOs at public companies reported having touchpoints with more functions, on average, and more often reported spending time with or consulting with the board, business unit leaders, and legal, compliance, and risk than their peers at private companies.

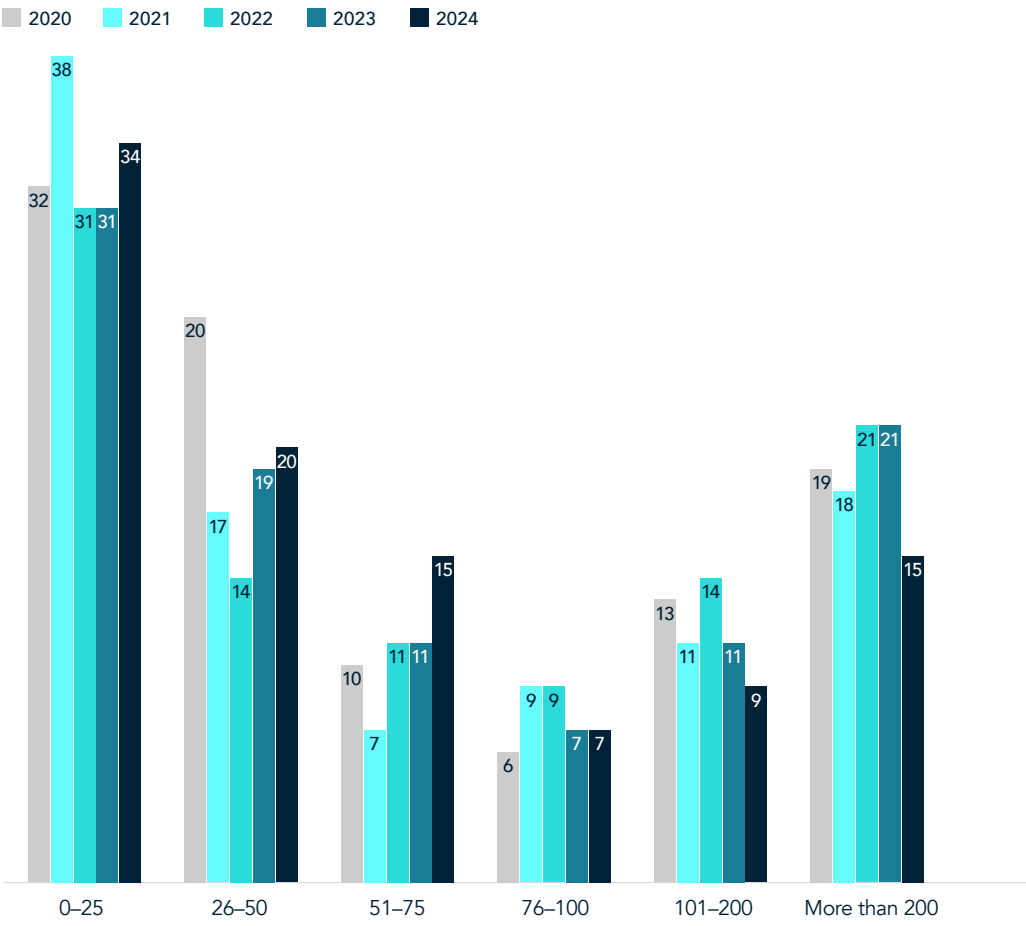
Functions with whom CISOs and their teams have any touchpoints, by ownership (%)



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 349

On the whole, respondents' team size seems to be shrinking year over year.

Team size, by year (%)



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 370; Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 242; Heidrick & Struggles' global chief information security officer (CISO) survey, 2022, n = 327; Heidrick & Struggles' global chief information security officer (CISO) survey, 2021, n = 354; Heidrick & Struggles' global chief information security officer (CISO) survey, 2020, n = 372

SIDEBAR

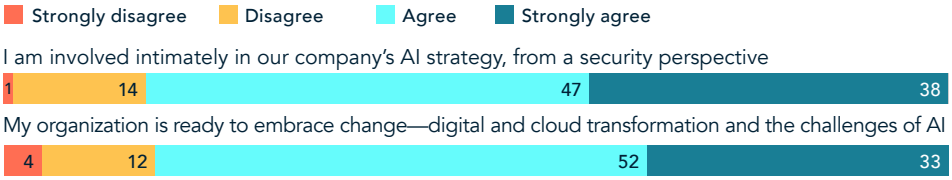
AI as a cyber and information security threat

How are cyber and information security officers talking about AI? What are their specific concerns? In our conversations with these leaders, we've found that there are four main themes:

1. How are we protecting what we're doing with AI internally?
2. How are we using AI to better protect the company? What AI cybersecurity tools are available to us?
3. How are adversaries using AI, and what can we do to protect against them?
4. How responsible is our use of AI? How trustworthy are these tools, and what governance should be put in place?

The good news is that respondents are already involved in these areas, and they are generally confident that their organizations are ready to embrace digital and cloud transformation, as well as the challenges of AI. In a recent survey of functional leaders about their organizations' use of AI, 40% of respondents said that the CEO is involved in setting AI policies.[2] Legal leaders are also involved. All this suggests that concerns about AI risks are being dealt with at the top.

To what extent do you agree with each of the following statements? (%)



Note: Numbers may not total 100% due to rounding.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 370

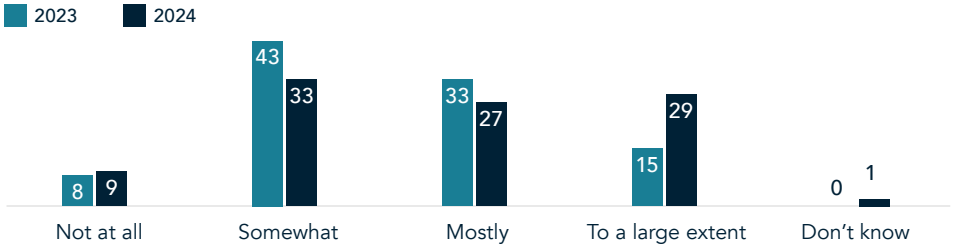
2 "How functional leaders are using AI—and barriers to progress," Heidrick & Struggles, heidrick.com.

SIDEBAR

The board landscape

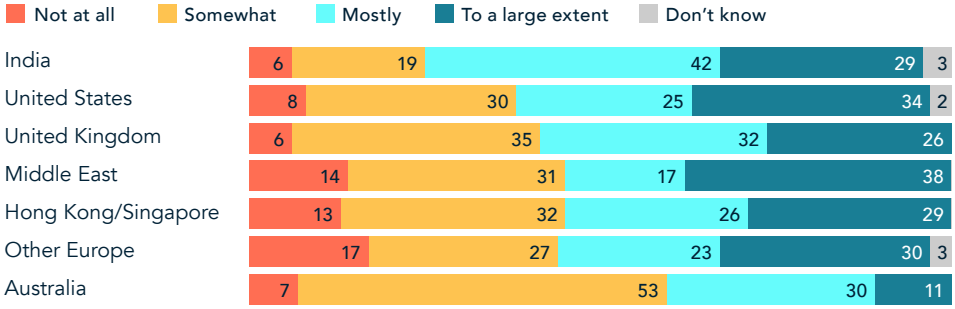
CISOs' confidence in the board seems to be growing, albeit slowly. When asked whether they think the board has the knowledge or expertise to respond effectively to cyber or information security presentations, a larger share of respondents this year said it does to a large extent. Respondents in India, the United States, and the United Kingdom are most confident in their boards.

Does the board have the knowledge or expertise to respond effectively to cyber presentations?, 2024 vs. 2023 (%)



Note: Numbers may not sum to totals due to rounding.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 362; Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 243

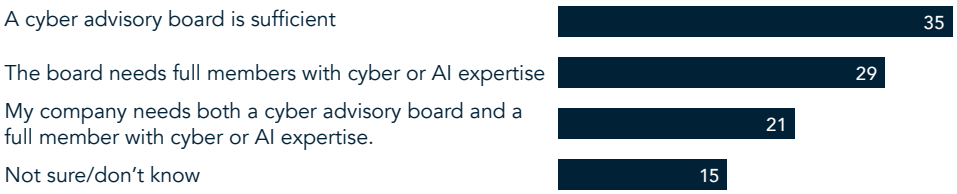
Does the board have the knowledge or expertise to respond effectively to cyber presentations?, by region (%)



Note: Numbers may not total 100% due to rounding.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 362

Globally, respondents most often said that a cyber advisory board is sufficient, as opposed to naming a full-time cybersecurity expert to the board.

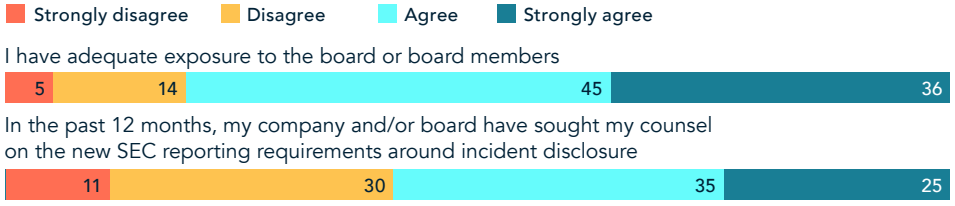
What type of board does your company need? (%)



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 361

Most respondents feel they have adequate exposure to the board, and more than half, 60%, said that their company or board has sought their counsel on new SEC reporting requirements for incident exposures.

To what extent do you agree with each of the following statements? (%)



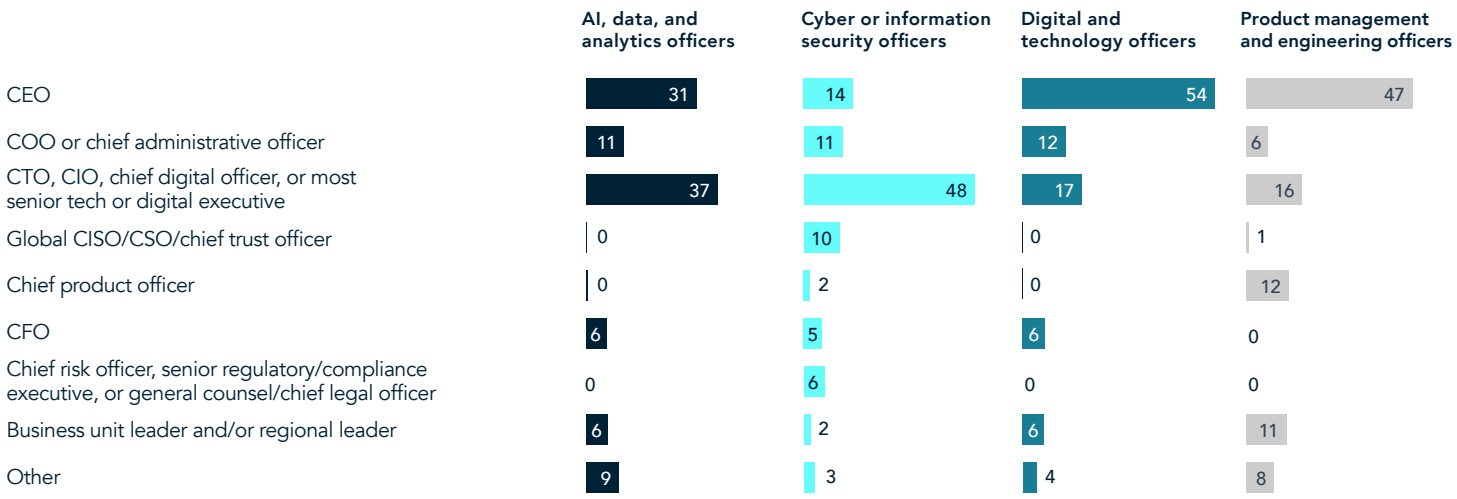
Note: Numbers may not total 100% due to rounding.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 370

SIDEBAR

A look across the tech landscape

Looking at our surveys of technology leaders across functions,[1] including AI, data, and analytics officers; digital, information, and technology officers; and product management or product engineering officers, it is cybersecurity officers who most often report to the CTO, CIO, chief digital officer, or the top digital, technology, or engineering officer, despite this year's drop.

To whom respondents report, by role (%)



Note: Numbers may not total 100% due to rounding.
Source: Heidrick & Struggles' global data, analytics, and artificial intelligence executive organization and compensation survey, 2024, n = 416; Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 408; Heidrick & Struggles' digital & technology officers organization and compensation survey, 2024, n = 372; and Heidrick & Struggles' chief product officer compensation survey, 2024, n = 152

As for where they spend their time, CISOs; data, analytics, and AI officers; and senior digital and technology leaders frequently spend time with software development, product development, and product engineering.

A higher share of CISOs report spending their time with network, cloud, and infrastructure, as well as legal, compliance, and risk.

Top five functions with whom respondents and their teams have any touchpoints, by role (%)

	AI, data, and analytics officers	Cyber or information security officers	Digital and technology officers	Product management and engineering officers
1	Software development/ product development/ product engineering	Network, cloud, infrastructure	Software development/ product development/ product engineering	Sales/go-to-market
2	Operations	Software development/ product development/ product engineering	Marketing and customer engagement	Marketing and customer engagement
3	Marketing and customer engagement	Legal/compliance/risk	Operations	Business unit/ P&L leaders
4	Strategy	Corporate IT applications	Sales/go-to-market	Strategy
5	Finance	Finance	Strategy	Design

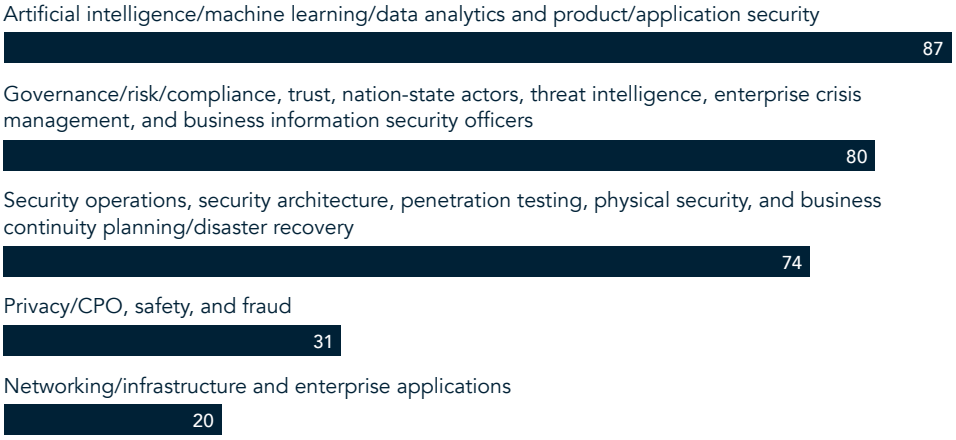
Source: Heidrick & Struggles' global data, analytics, and artificial intelligence executive organization and compensation survey, 2024, n = 396; Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 362; Heidrick & Struggles' digital & technology officers organization and compensation survey, 2024, n = 343; and Heidrick & Struggles' chief product officer compensation survey, 2024, n = 141

1 This year, Heidrick & Struggles surveyed not only cybersecurity or information security officers but also AI, data, and analytics officers; digital, information, and technology officers; and product management or product engineering officers. Reports for each survey are forthcoming on heidrick.com.

Building and maintaining expertise for the future

Looking to the future, CISOs selected an average of five areas in which it will be important to build or maintain expertise over the next five years. Unsurprisingly, they most often chose AI, machine learning, and data analytics and product and application security.

Where is it most important to build or maintain expertise over the next 3–5 years? (%)



Note: Respondents could select more than one response.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 371

By region, there are several notable callouts:

- Respondents in Australia most often said that business continuity and disaster planning were important areas in which to build or maintain expertise over the next three to five years, as well as penetration testing.
- A notably high share of respondents in Europe said that enterprise crisis management was an important area.
- Respondents in India least often named penetration testing and fraud as important areas in the near future.

Where is it important to build or maintain expertise over the next 3–5 years?, by region (%)

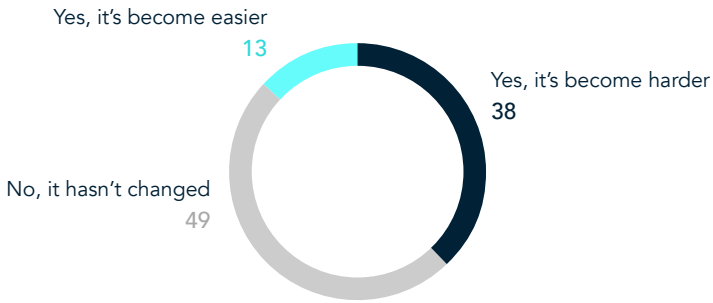
	Australia	Middle East	Hong Kong/ Singapore	India	Other Europe	United Kingdom	United States
Artificial intelligence/machine learning/data analytics	84	72	65	77	74	68	83
Security operations	62	41	61	52	55	42	51
Governance, risk, and compliance	41	45	58	39	55	42	51
Security architecture	64	38	48	45	58	35	43
Product/application security	52	55	29	39	35	32	50
Nation-state actors/threat intelligence	45	21	39	32	32	19	36
Business continuity planning/ disaster recovery	50	17	39	29	26	16	26
Enterprise crisis management	29	28	13	29	52	23	26
Trust	14	28	16	39	32	26	29
Penetration testing	41	24	13	3	19	13	18
Privacy/CPO	21	17	13	23	23	6	19
Fraud	21	24	13	10	19	16	16
Networking/infrastructure	16	21	10	10	23	13	12
Business information security officers	16	10	16	3	19	19	13
Enterprise applications	5	17	6	19	10	16	13
Physical security	12	7	3	6	6	6	7
Safety	10	7	6	3	6	3	5
Other	7	3	0	0	6	13	6

Note: Respondents could select more than one response.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 371

The talent landscape

Looking at the future of talent, almost half of respondents said that the recruiting landscape hasn't changed in the past 12 months, but more than one-third said it has changed—by becoming more challenging. Compensation was the challenge most often cited when recruiting new talent.

Has the ease of recruiting new talent changed in the past 12 months? (%)



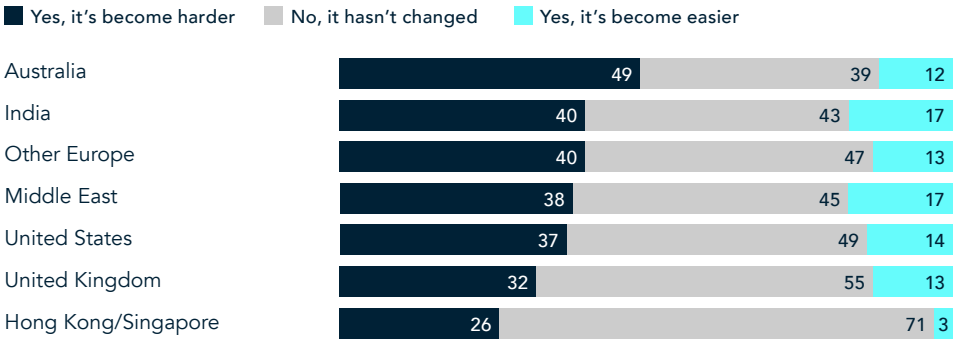
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 363

Biggest challenges in recruiting new talent (%)

Note: Respondents could select more than one response.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 361

In addition to compensation, respondents in Australia and those in Hong Kong and Singapore also cited company industry far more than their peers in other regions, and UK respondents more often than their peers cited a lack of interest among current employees in reskilling in other areas. More than half of respondents in Europe, and 46% of US respondents, cited company location as a challenge.

Has the ease of recruiting new talent changed in the past 12 months?, by region (%)



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 363

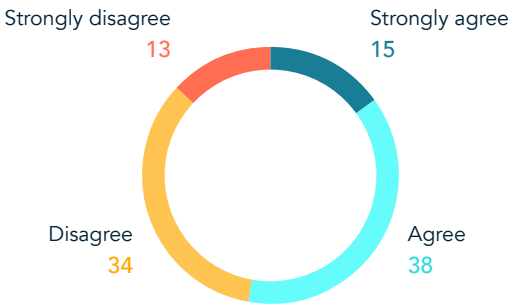
Biggest challenges in recruiting new talent, by region (%)

	Australia	Middle East	Hong Kong/ Singapore	India	Other Europe	United Kingdom	United States
Compensation	86	76	58	60	75	83	78
Job location	30	31	29	40	54	37	46
Too much stress in the role	37	31	32	30	32	27	29
Culture fit with the company and/or team	33	21	23	33	36	23	25
Perception of company or product in the market	19	17	19	33	11	17	19
Company industry	26	7	23	7	7	7	9
Lack of interest among current employees in reskilling in other areas	11	0	10	10	7	20	7
Fear of career risk as a result of a breach	4	7	10	10	0	10	9
Other	12	7	10	3	18	17	12

Note: Respondents could select more than one response.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 361

Looking ahead, just over half, 53%, of respondents agreed that they have an internal successor in place who is just as good as or better than the external market can present.

To what extent do you agree or disagree with the following statement?: I have a successor in place who I feel is just as good as or better than the external market can present (%)



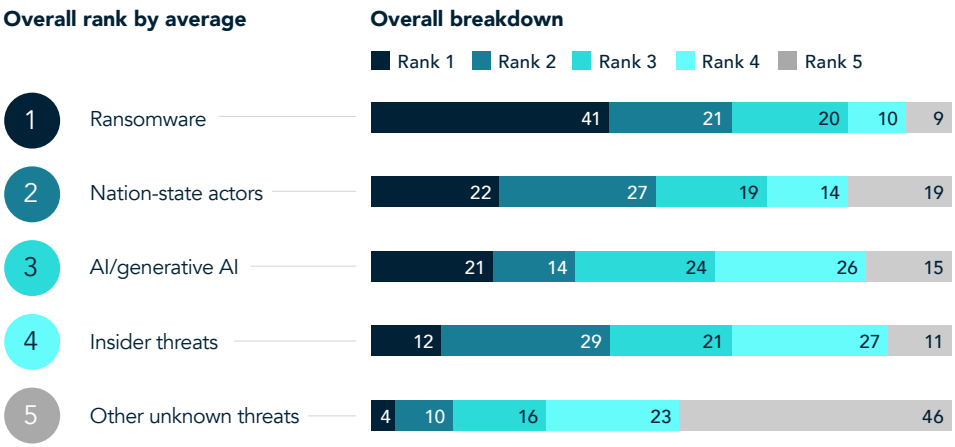
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 370

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, this year we asked again about the risks, both personal and professional, that CISOs face in their role. Unsurprisingly, the most often cited cybersecurity risk was ransomware, followed by geopolitical risks, such as nation-state actors, and then AI.

Cybersecurity threats (%)



Note: Numbers may not total 100% due to rounding.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 362

By region, respondents in the United Kingdom most often cited ransomware as a top threat, and least often cited nation-state actors.

Respondents in India least often cited ransomware as a top threat, and most often cited AI.

Cybersecurity threats, by region (%)

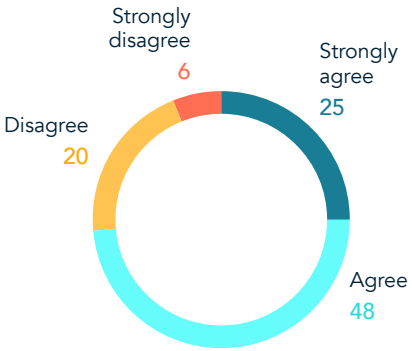
	Australia	Middle East	Hong Kong/ Singapore	India	Other Europe	United Kingdom	United States
Ransomware	44	34	39	26	50	61	38
Nation-state actors	21	21	35	19	30	6	23
AI/generative AI	21	24	13	32	13	13	22
Insider threats	7	14	10	19	3	16	13
Other unknown threats	7	7	3	3	3	3	4

Note: Numbers may not total 100% due to rounding.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 362

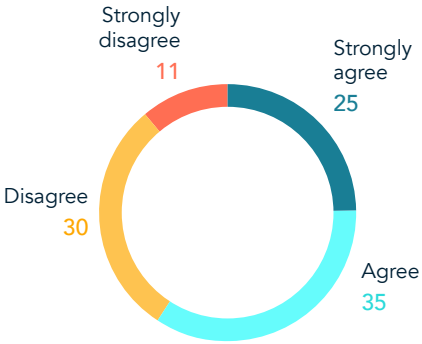
Most respondents felt that their organization accurately characterized in its public filings how much cyberrisk it faces, and that their organization has provided them with enough resources to meet security expectations.

To what extent do you agree or disagree with the following statements?: (%)

I feel that my company accurately characterizes in our public findings how much cyberrisk we face



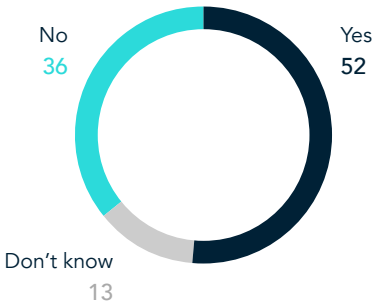
For the current budget period, I have received enough resources (talent, money, etc.) to meet the expectations of my organization



Note: Numbers may not total 100% due to rounding.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 370

Still, there are other steps that can be taken to protect information security officers from liability. This year, 52% of respondents said that they are covered by D&O insurance, up from 44% in 2023.

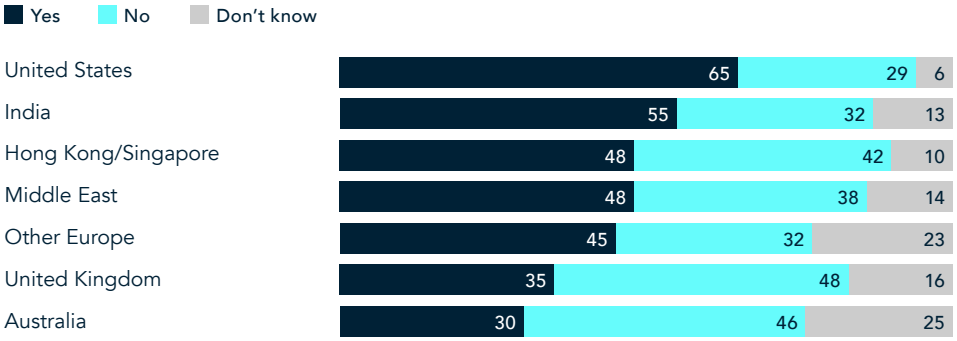
Are you covered by your company's D&O insurance? (%)



Note: Numbers may not total 100% due to rounding.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 369

US respondents are most often covered by their company's D&O insurance. However, the recent dismissal of an SEC lawsuit against the software company SolarWinds in the wake of a Russia-linked cyberattack targeting the US government could be interpreted as a win for CISOs and their liability.[3] Despite this development, we anticipate that many cyber and information security leaders will still want insurance, as a precaution.

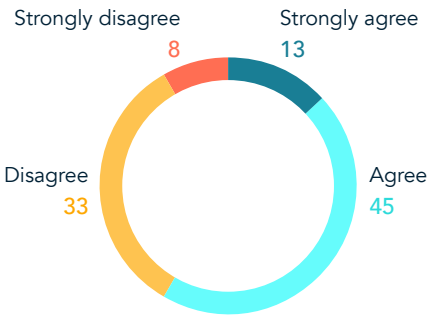
Are you covered by your company's D&O insurance?, by region (%)



Note: Numbers may not total 100% due to rounding.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 369

However, across the map, more than half of respondents do not think that D&O will protect them from personal liability in the event of a breach.

To what extent do you agree or disagree with the following statement?: D&O insurance will not protect me from personal liability in the event of a breach (%)



Note: Numbers may not total 100% due to rounding.
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 370

3 Jonathan Stempel, "SolarWinds beats most of US SEC lawsuit over Russia-linked cyberattack," Reuters, July 18, 2024, reuters.com.

The state of CISO compensation

Global

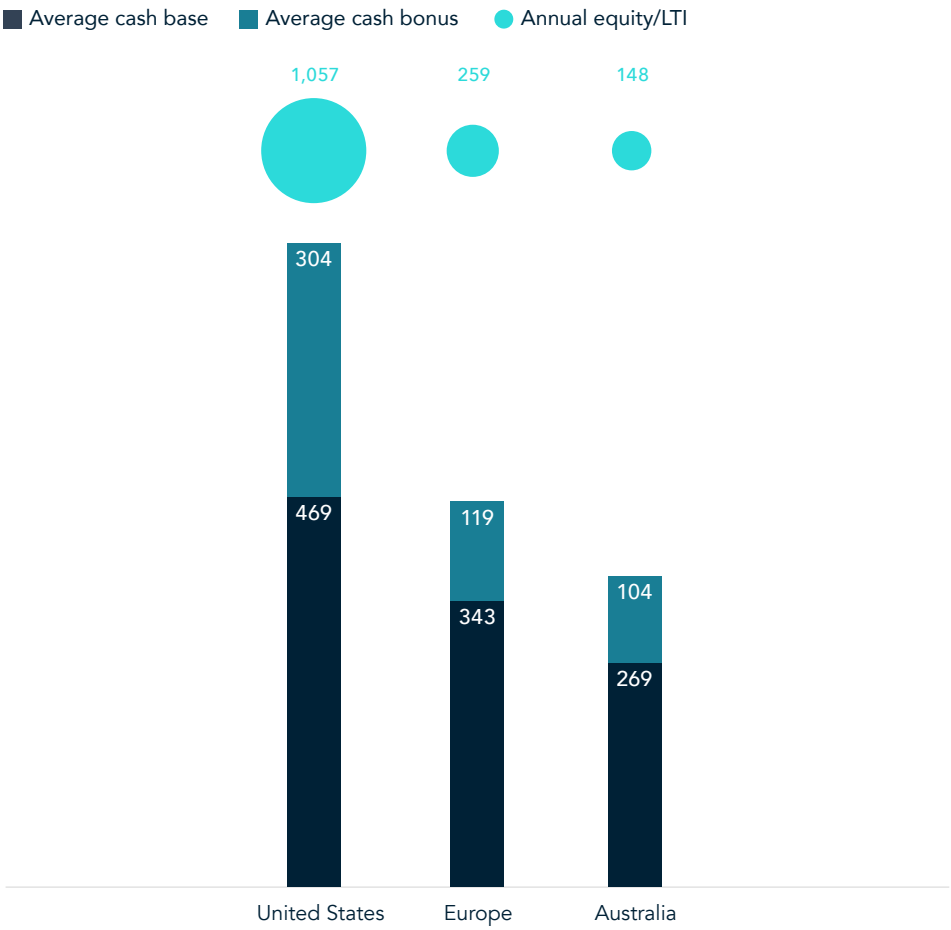
Comparing regions, cyber and information security officers in the Middle East and the United States reported the highest average base compensation, at $498,000 and $468,000, respectively. Respondents in Australia reported the lowest average base compensation, at $269,000.

Respondents in the United States and India reported the highest average annual equity/LTI, at $1,057,000 and $826,000, respectively.

Respondents in the United States, India, and the Middle East reported the highest average sign-on cash, and respondents from the United States and India reported the highest average sign-on equity.

In Australia, Europe, and Hong Kong and Singapore, respondents at financial services firms generally reported the highest average compensation, while respondents at consumer companies in India and the United States reported the highest compensation for their regions.

Global compensation trends, 2024 (USD thousands)

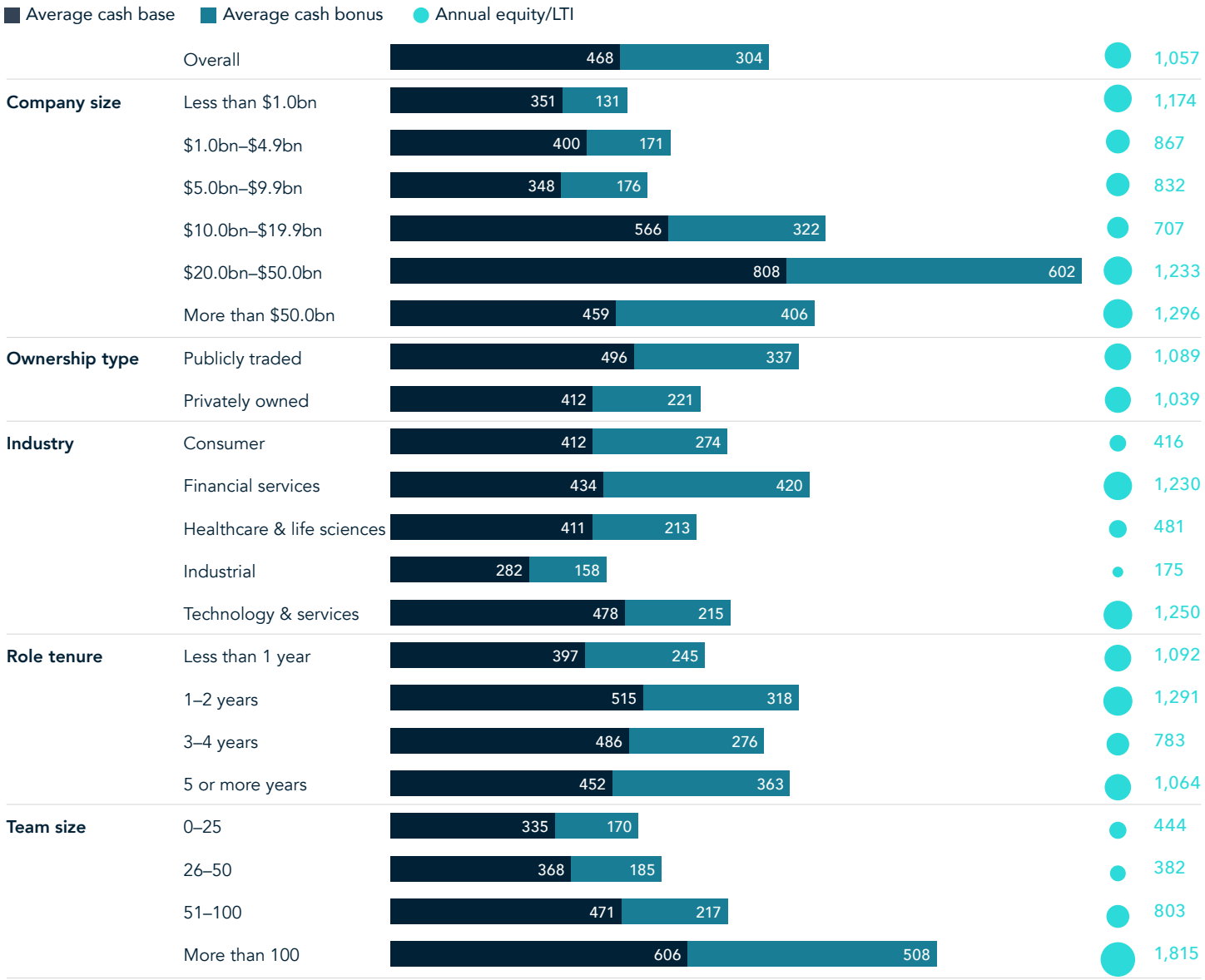


Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 261

CISO compensation: United States

Respondents in the United States reported an average cash base of $468,000 and an average cash bonus of $304,000. Respondents at consumer companies saw notably higher compensation than their peers, as did respondents with larger team sizes and at companies with between $20 billion and $50 billion in revenue.

United States compensation trends: Snapshot (USD thousands)



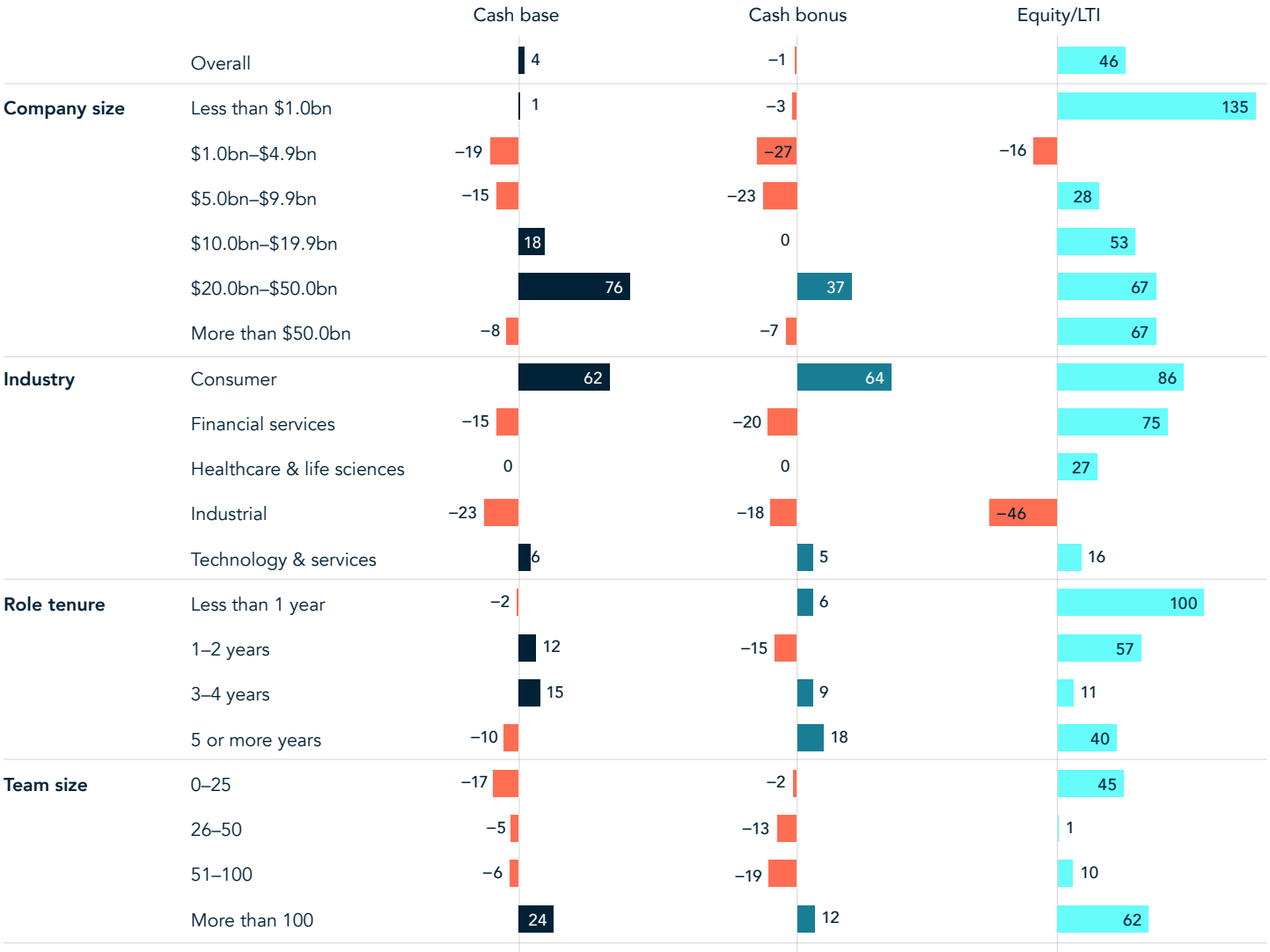
Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 151
Note: Average cash bonus and average equity/LTI only include those who reported receiving that type of compensation.

Year over year, average cash base and bonus for US respondents varied by industry, tenure, and company size. Equity/LTI trended up across all respondents.

Equity/LTI increased substantially year over year for respondents from smaller companies, those with less than $1 billion in revenue, as well as for respondents with less than a year in their current role, pointing to the significant cost of replacing these executives and the importance of retention and succession planning.

Respondents at consumer companies in particular saw significant year-over-year increases across average base, bonus, and equity.

United States year-over-year compensation trends: Growth (%)



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 151; Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 149

United States compensation trends: Snapshot (USD thousands)

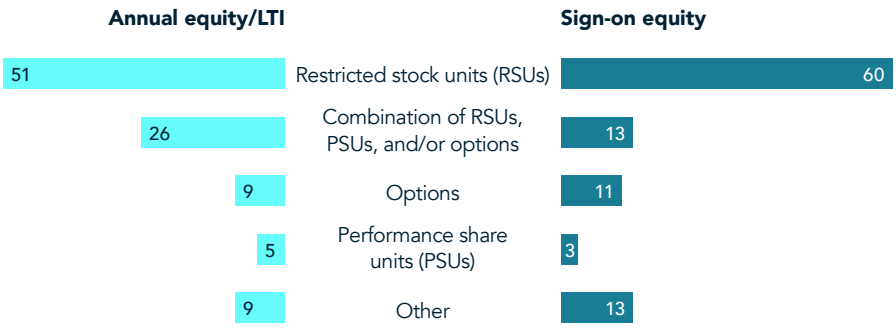
		n	Cash base				Cash bonus				Total cash compensation				Equity/LTI				Total compensation (including equity)			
			25th	avg.	75th	95th	25th	avg.	75th	95th	25th	avg.	75th	95th	25th	avg.	75th	95th	25th	avg.	75th	95th
	Overall	151	320	469	500	750	100	304	400	850	410	738	810	1,400	200	1,057	1,000	4,000	640	1,648	1,910	5,100
Company size	Less than $1.0bn	38	300	351	400	500	80	131	160	300	380	454	530	700	200	1,174	1,000	3,000	490	1,350	1,390	3,660
	$1.0bn–$4.9bn	20	330	400	428	883	90	171	200	500	435	563	675	1,374	310	867	1,000	4,000	745	1,343	1,773	4,550
	$5.0bn–$9.9bn	13	300	348	400	440	105	176	238	340	400	510	590	710	80	832	1,300	3,000	460	1,214	1,200	3,590
	$10.0bn–$19.9bn	20	350	566	500	3,360	180	322	500	700	548	872	1,000	3,509	180	707	500	5,800	750	1,578	1,800	6,444
	$20.0bn–$50.0bn	17	350	808	700	5,100	148	602	700	2,200	600	1,375	1,300	7,200	170	1,233	1,100	7,860	930	2,463	3,000	10,810
	More than $50.0bn	34	390	459	530	800	240	406	550	1,000	500	805	1,100	1,500	310	1,296	1,300	4,500	800	1,910	2,500	5,530
Ownership type	Publicly traded	100	305	496	500	750	105	337	400	1,000	430	806	830	1,529	220	1,089	1,000	4,500	755	1,840	2,100	5,825
	Privately owned	47	310	412	500	800	100	221	300	650	400	591	700	1,200	200	1,039	1500	4,000	490	1,277	1,550	3,800
Industry	Consumer	10	280	412	550	700	100	274	330	700	340	659	880	1,400	63	416	875	1,000	430	992	1,800	1,900
	Financial services	49	350	435	500	700	160	420	500	1,000	550	837	1,000	1,500	200	1,230	1,000	4,500	720	1,891	2,200	5,840
	Healthcare & life sciences	17	360	411	470	550	100	213	288	400	460	612	790	950	250	481	700	1,250	500	1,037	1,350	2,040
	Industrial	12	210	282	338	390	100	158	240	250	293	413	565	590	100	175	250	350	443	573	773	940
	Technology & services	60	320	478	438	850	90	215	260	600	403	657	648	1,485	330	1,250	2,000	4,000	773	1,720	2,300	5,076
Role tenure	Less than 1 year	20	305	397	480	834	120	245	350	600	480	630	823	1,110	250	1,092	1,500	4,000	660	1,558	1,973	5,025
	1–2 years	43	310	515	500	700	100	318	310	1,000	400	796	700	1,500	200	1,291	1,075	6,000	570	1,876	2,100	6,540
	3–4 years	38	290	486	500	1,450	100	276	360	700	380	711	790	2,810	300	783	1,000	2,000	450	1,371	1,650	4,620
	5 or more years	42	370	452	500	800	150	363	440	1,100	470	780	880	1,400	220	1,064	1,000	4,500	810	1,717	1,880	3,800
Team size	0–25	40	250	335	400	595	80	170	180	500	318	479	568	1,087	110	444	400	1,500	400	779	958	2,096
	26–50	23	310	368	400	500	100	185	250	310	380	545	700	800	150	382	500	1,000	560	894	1,000	1,550
	51–100	33	330	471	400	530	120	217	280	400	490	668	710	1,150	220	803	1,000	3,000	800	1,422	1,450	4,600
	More than 100	55	430	606	600	900	243	508	688	1,360	600	1,050	1,200	2,810	400	1,815	2,500	6,000	1,100	2,732	3,420	8,300

Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 151
Note: Average cash bonus and average equity/LTI only include those who reported receiving that type of compensation.

More than half, 51%, of US respondents said that their annual equity/LTI comes in the form of restricted stock units.

As for sign-on equity, 60% reported that their sign-on equity was also in the form of restricted stock units.

United States: Format of equity (%)



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, annual equity/LTI: n = 140; sign-on equity: n = 96

Respondents' average sign-on cash was $290,000, and average sign-on equity was $783,000.

United States compensation trends: Sign-on bonus (USD thousands)

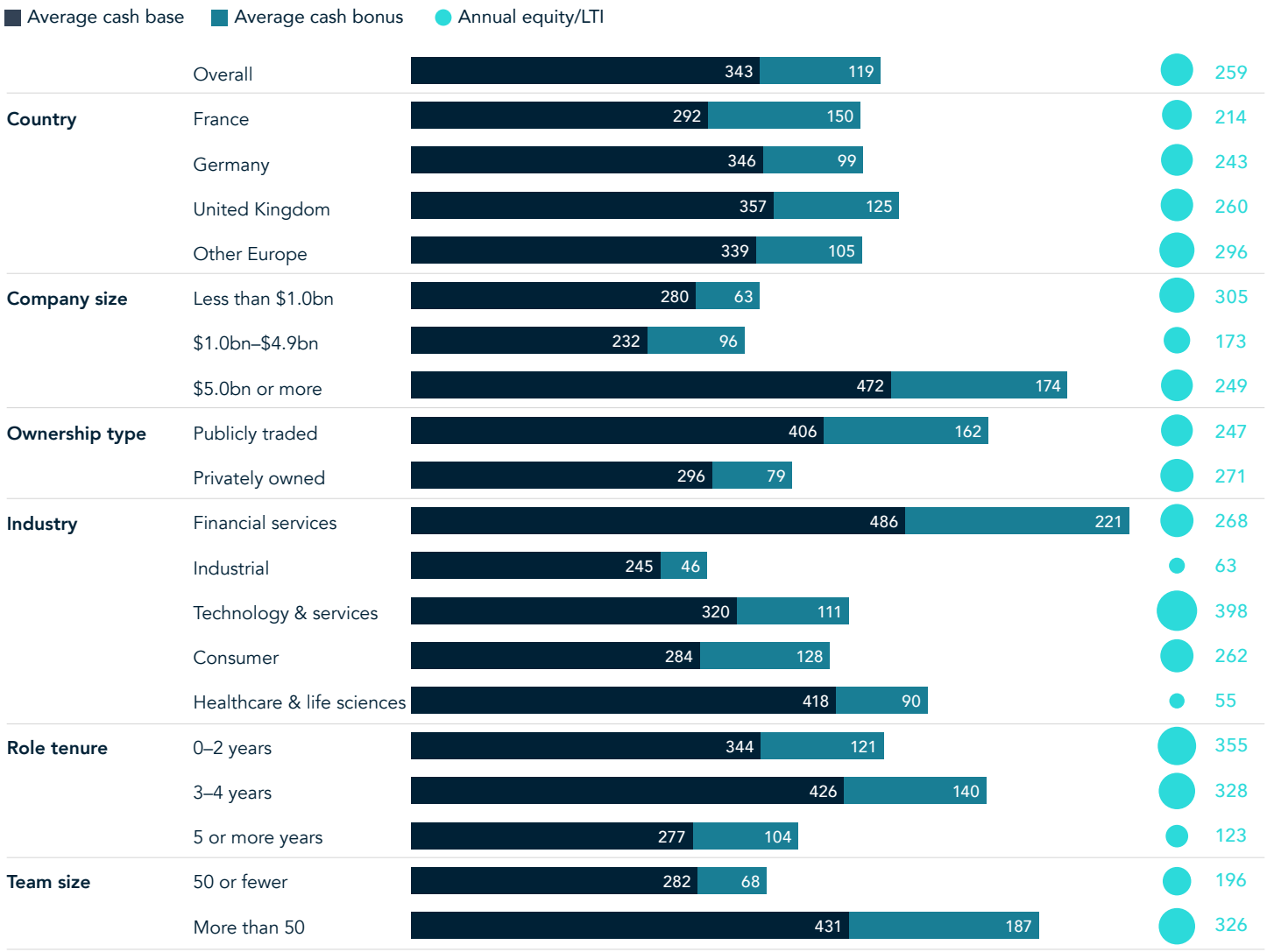
		n	Sign-on: Cash				Sign-on: Equity			
			25th	avg.	75th	95th	25th	avg.	75th	95th
	Overall	99	80	290	330	1,000	230	783	1,000	2,800
Company size	Less than $1.0bn	22	30	164	153	1,200	250	791	950	2,800
	$1.0bn–$4.9bn	14	50	177	200	780	200	1,336	1,500	5,000
	$5.0bn–$9.9bn	10	63	138	200	250	250	571	800	1,500
	$10.0bn–$19.9bn	16	100	275	350	1,000	148	541	1,225	1,500
	$20.0bn–$50.0bn	10	200	574	875	2,010	300	851	1,000	2,100
	More than $50.0bn	21	200	407	500	1,000	300	739	1,000	4,000
Ownership type	Publicly traded	68	100	344	500	1,000	230	807	1,000	2,800
	Privately owned	28	50	176	200	780	300	800	800	4,000
Industry	Consumer	9	50	273	500	1,000	400	720	500	2,100
	Financial services	32	100	290	400	1,000	300	1,151	1,500	5,000
	Healthcare & life sciences	13	48	185	250	400	208	391	375	1,300
	Industrial	7	100	122	150	200	200	280	400	500
	Technology & services	38	70	363	500	1,200	250	762	1,000	2,000
Role tenure	Less than 1 year	12	50	179	300	500	300	750	1,500	1,500
	1–2 years	29	53	303	438	1,000	230	689	650	2,800
	3–4 years	26	100	316	300	2,010	200	813	1,000	4,000
	5 or more years	25	100	295	500	700	250	695	500	4,000
Team size	0–25	25	50	147	100	1,200	200	411	500	800
	26–50	11	30	86	100	300	130	872	500	4,000
	51–100	24	60	194	250	780	200	747	800	5,000
	More than 100	39	200	468	500	1,000	300	916	1,300	2,800

Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 99

CISO compensation: Europe

Respondents in Europe (including the United Kingdom) reported an average cash base of $343,000 and an average cash bonus of $119,000. Respondents at financial services companies saw notably higher compensation than their peers, as did respondents with larger team sizes, from public companies, and at companies with $5 billion or more in revenue.

Europe compensation trends: Snapshot (USD thousands)



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 54
Note: Average cash bonus and average equity/LTI only include those who reported receiving that type of compensation.

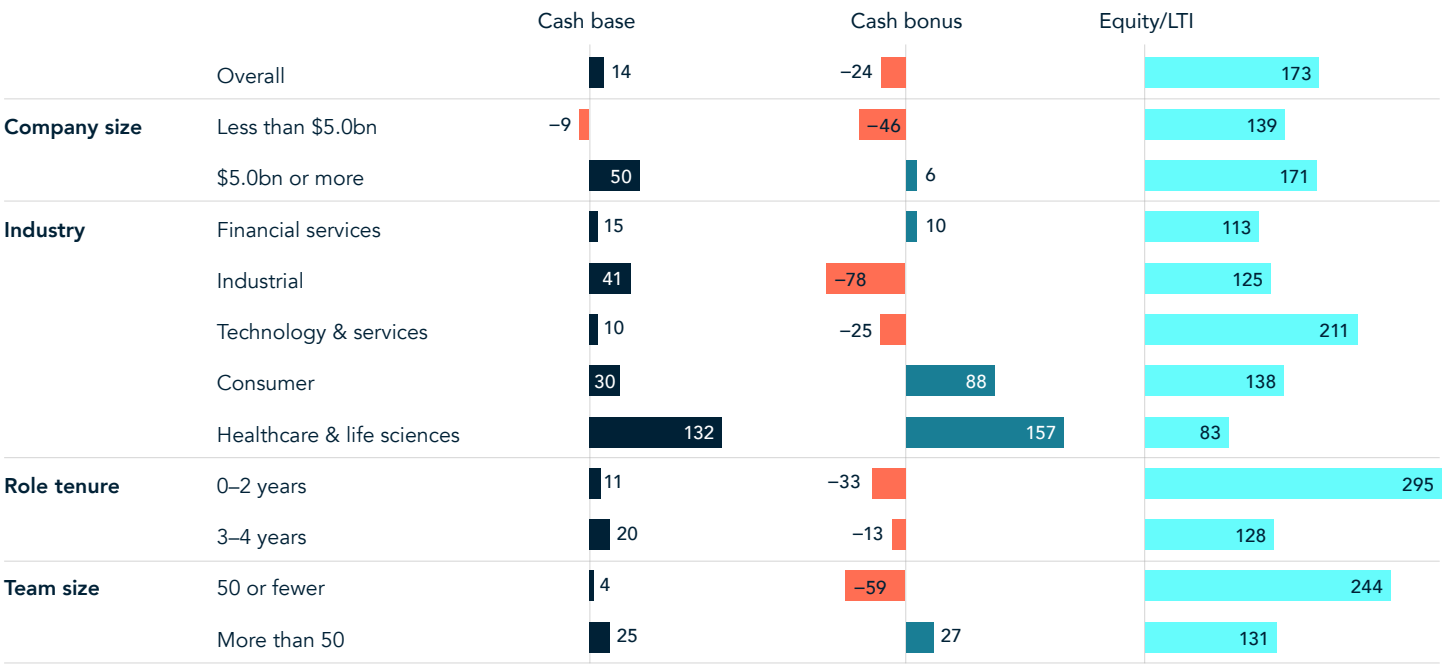
Europe compensation trends (USD thousands)

		n	Cash base			Cash bonus			Total cash compensation			Equity/LTI			Total compensation (including equity)		
			25th	avg.	75th	25th	avg.	75th	25th	avg.	75th	25th	avg.	75th	25th	avg.	75th
	Overall	54	160	343	400	30	119	200	183	432	583	60	259	300	218	595	828
Country	France	6	130	292	440	40	150	50	180	417	440	100	214	300	280	595	740
	Germany	10	120	346	300	10	99	80	150	415	300	100	243	300	150	561	580
	United Kingdom	27	183	357	400	33	125	200	190	442	590	60	260	300	240	584	850
	Other Europe	11	140	339	400	30	105	200	170	435	600	40	296	400	210	650	1,060
Company size	Less than $1.0bn	24	150	280	360	30	63	60	180	319	410	63	305	450	190	487	700
	$1.0bn–$4.9bn	11	150	232	300	30	96	120	170	305	440	40	173	120	200	414	500
	$5.0bn or more	19	200	472	500	30	174	250	240	637	720	100	249	300	280	821	1,100
Ownership type	Publicly traded	22	200	406	470	33	162	250	240	553	650	60	247	300	280	767	1,000
	Privately owned	32	150	296	400	30	79	100	170	344	440	60	271	300	190	469	700
Industry	Financial services	11	270	486	500	150	221	250	370	685	720	100	268	400	430	941	1,100
	Industrial	11	140	246	300	30	46	50	170	287	410	40	63	90	190	327	480
	Technology & services	18	200	320	400	30	111	100	240	394	440	100	398	575	280	660	890
	Consumer	8	200	284	400	25	128	238	240	357	600	40	262	250	280	439	700
	Healthcare & life sciences	6	40	418	180	13	90	233	40	478	190	10	55	100	50	497	270
Role tenure	0–2 years	22	150	344	400	30	121	250	180	431	500	100	356	600	200	569	850
	3–4 years	14	250	426	500	33	140	205	260	546	650	70	328	450	280	827	1,060
	5 or more years	16	150	277	360	30	104	100	170	355	440	45	123	115	190	446	580
Team size	50 or fewer	32	140	282	300	23	68	75	170	336	310	40	196	300	190	422	440
	More than 50	22	260	431	470	60	187	250	310	564	650	100	326	400	410	831	1,100

Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 54
Note: Average cash bonus and average equity/LTI only include those who reported receiving that type of compensation.

Year over year, average base compensation and equity/LTI for respondents in Europe generally trended up, while bonuses trended down. Respondents at healthcare and life sciences companies in particular saw significant year-over-year increases across average base, bonus, and equity.

Europe year-over-year compensation trends: Growth (%)

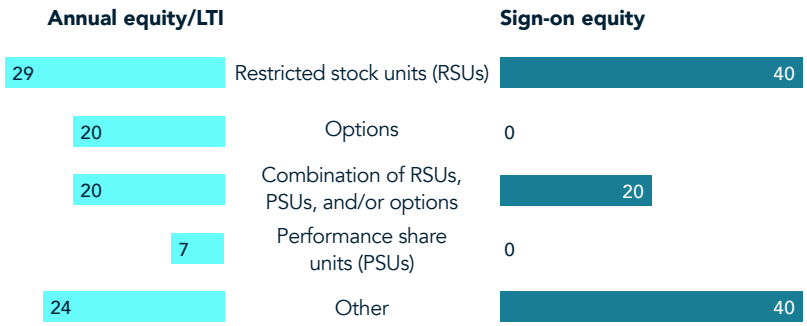


Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 54; Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 38

Twenty-nine percent of respondents in Europe said that the format of their annual equity/LTI comes in the form of restricted stock units. Nearly a quarter named other formats.

As for sign-on equity, 40% reported that this equity also came in the form of restricted stock units.

Europe: Format of equity (%)



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, annual equity/LTI: n = 41; sign-on equity: n = 25

Of the respondents in Europe, those at smaller companies, those with less than $1 billion in revenue, received the highest average sign-on cash bonus and equity. Those at privately owned companies also outperformed their peers.

Europe compensation trends: Sign-on bonus (USD thousands)

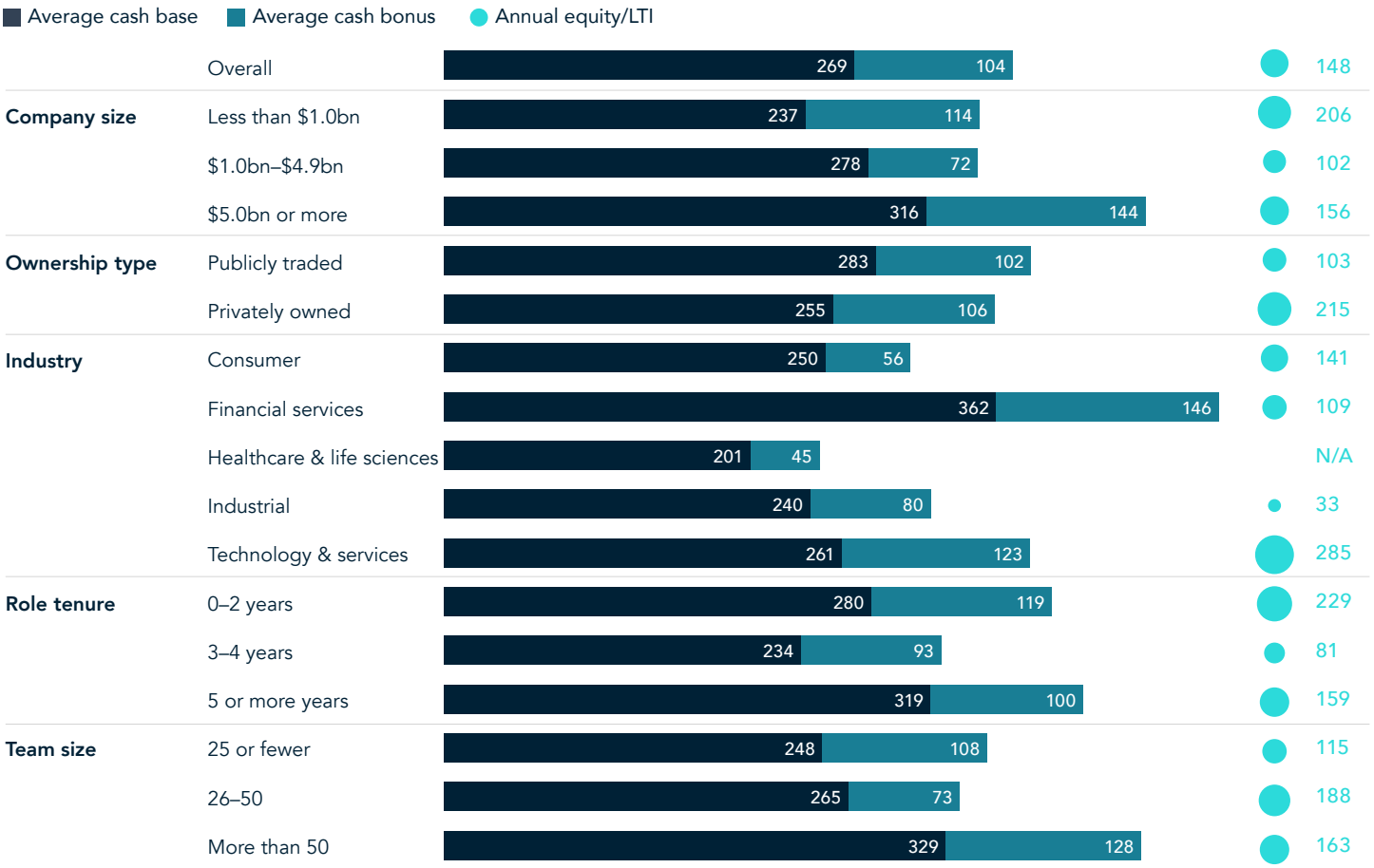
		n	Sign-on: Cash			Sign-on: Equity		
			25th	avg.	75th	25th	avg.	75th
	Overall	21	40	186	200	200	549	700
Country	France	4	25	215	530	50	600	1,250
	Germany	5	30	153	388	20	273	500
	United Kingdom	8	100	128	158	80	537	1,000
	Other Europe	4	200	267	400	200	738	1,638
Company size	Less than $1.0bn	10	30	210	350	200	715	1,188
	$1.0bn–$4.9bn	2	150	155	160	80	390	700
	$5.0bn or more	9	50	158	100	80	404	500
Ownership type	Publicly traded	11	40	147	160	80	401	500
	Privately owned	10	48	219	350	200	715	1,188
Industry	Financial services	5	200	300	500	200	460	500
	Industrial	3	30	280	660	20	200	500
	Technology & services	9	40	130	160	80	704	1,250
	Consumer	3	30	65	100	N/A	N/A	N/A
	Healthcare & life sciences	1	N/A	N/A	N/A	500	500	500
Role tenure	0–2 years	7	140	167	200	500	743	1,000
	3–4 years	7	100	233	400	80	543	500
	5 or more years	5	33	208	520	28	218	450
Team size	50 or fewer	9	30	90	150	80	379	550
	More than 50	12	100	233	400	200	668	1,000

Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 21

CISO compensation: Australia

Respondents in Australia reported an average cash base of $269,000 and an average cash bonus of $104,000. Respondents at financial services companies saw notably higher compensation than their peers, as did respondents with larger team sizes.

Australia compensation trends: Snapshot (USD thousands)



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 56
Note: Average cash bonus and average equity/LTI only include those who reported receiving that type of compensation.

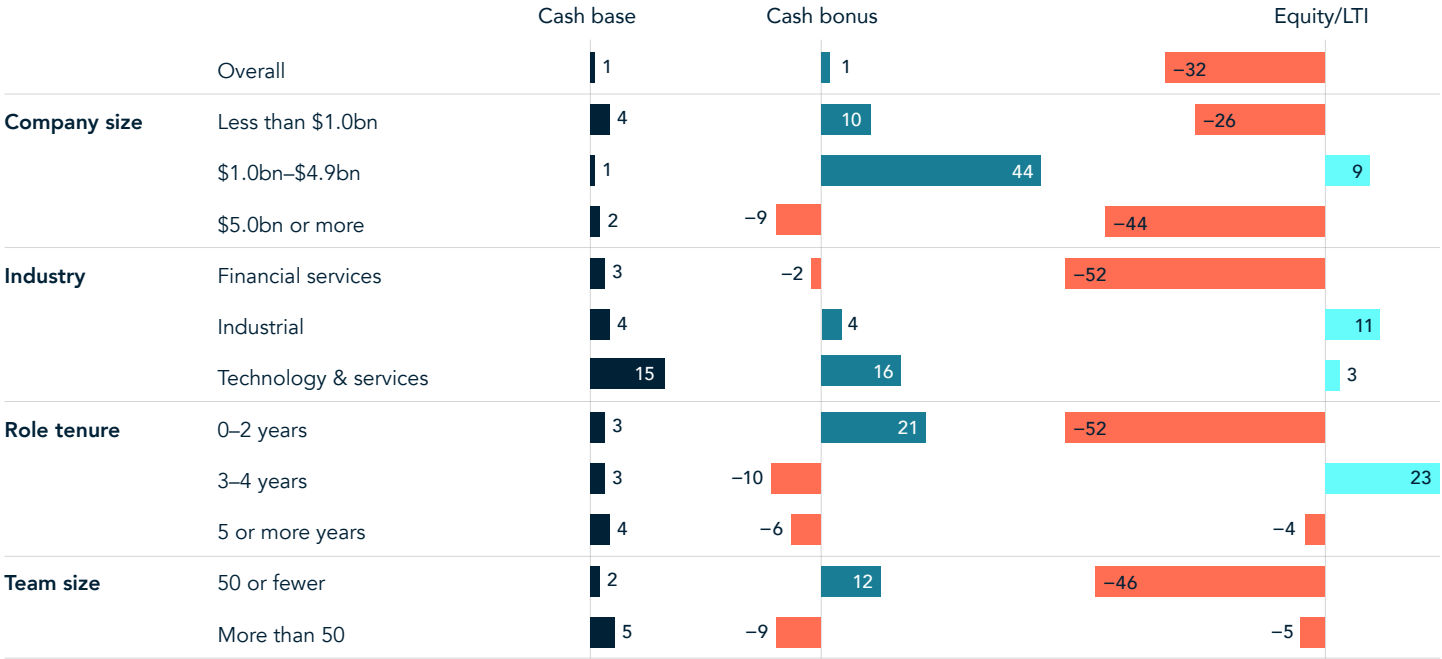
Australia compensation trends (USD thousands)

		n	Cash base			Cash bonus			Total cash compensation			Equity/LTI			Total compensation (including equity)		
			25th	avg.	75th	25th	avg.	75th	25th	avg.	75th	25th	avg.	75th	25th	avg.	75th
	Overall	56	200	269	300	43	104	120	223	343	413	50	148	200	243	414	533
Company size	Less than $1.0bn	18	200	237	300	40	114	200	210	301	390	60	206	350	220	392	540
	$1.0bn–$4.9bn	20	203	278	308	40	72	100	243	339	403	50	102	150	275	405	595
	$5.0bn or more	13	210	316	330	50	144	250	260	427	450	30	156	250	260	487	780
Ownership type	Publicly traded	28	200	283	318	30	102	110	223	366	410	30	103	188	243	425	580
	Privately owned	28	200	255	300	50	106	120	228	320	413	150	215	250	228	404	533
Industry	Consumer	13	200	250	310	23	56	88	200	285	340	50	141	250	230	361	490
	Financial services	12	235	362	423	50	146	250	285	496	638	50	109	170	363	596	773
	Healthcare & life sciences	7	180	201	220	20	45	70	180	214	260	N/A	N/A	N/A	180	214	260
	Industrial	10	210	240	260	38	80	115	250	304	350	20	33	50	270	314	350
	Technology & services	14	200	261	300	90	123	200	260	358	450	150	285	400	260	480	630
Role tenure	0–2 years	22	220	280	300	50	119	150	250	356	350	50	229	400	250	428	510
	3–4 years	23	180	234	300	23	93	120	200	299	380	20	81	150	200	334	410
	5 or more years	11	250	319	400	50	100	100	300	410	500	90	159	200	360	555	690
Team size	25 or fewer	32	185	248	300	50	108	120	200	312	350	50	115	200	203	352	468
	26–50	12	225	265	300	40	73	90	290	332	335	50	188	150	290	410	428
	More than 50	12	220	329	400	90	128	150	243	436	515	30	163	250	255	585	795

Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 56
Note: Average cash bonus and average equity/LTI only include those who reported receiving that type of compensation.

Year over year, average cash base and bonus compensation for respondents in Australia trended modestly up, but there were some significant decreases, mostly in equity/LTI.

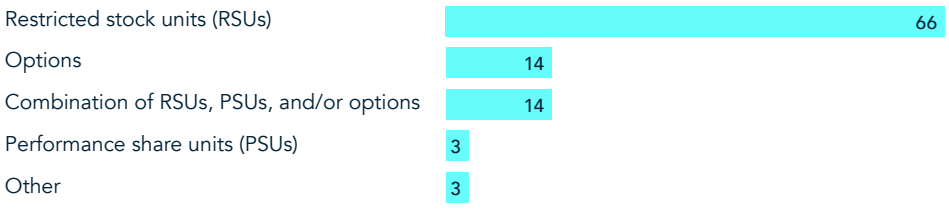
Australia year-over-year compensation trends: Growth (%)



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 56; Heidrick & Struggles' global chief information security officer (CISO) survey, 2023, n = 37

Two-thirds of respondents in Australia said that the format of their annual equity/LTI comes in the form of restricted stock units.

Australia: Format of annual equity/LTI (%)



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2024, n = 29

Specialty Practices

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

These practices include:

- Artificial Intelligence, Data & Analytics
- Crypto & Digital Assets
- Cybersecurity
- Health Tech
- Industrial Tech

Leader of Heidrick & Struggles' Specialty Practices

Global

Sam Burman
London
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

Katherine Graham Shannon
San Francisco
kshannon@heidrick.com