IANS + ARTICO

State of the CISO, 2023–2024

Benchmark Summary Report

© 2024 IANS, Artico Search. All rights reserved. For more information, write to info@iansresearch.com.

Table of Contents

This summary report provides high-level insights from our State of the CISO, 2023–2024 Benchmark Report.

The complete State of the CISO, 2023–2024 report is a comprehensive, 18-page breakdown that offers a more detailed set of data and is available to IANS clients through the IANS Portal or to non-clients upon request by contacting us at info@iansresearch.com

© 2024 IANS, Artico Search. All rights reserved. For more information, write to info@iansresearch.com.

Executive Summary

At the outset of 2024, the state of the CISO reflects a duality of both anxiety and opportunity.

This duality became evident during our recent discussions with about 100 prominent CISOs from across the U.S. and Canada. They attribute it to the culmination of major events:

First: Financial markets were volatile and inflation rose, prompting many companies to pull back on spending, including for their cybersecurity programs.

Meanwhile: Cyber breaches, ransomware attacks and overall threat alert levels increased, due to growing geopolitical instability and the evolving threat environment, in general.

Next: The unprecedented rise of generative AI tools that offer CISOs new opportunities for advanced threat detection, automation and adaptive defenses, but also pose new threats in themselves, as well as an expanded attack surface.

Last: The SEC and regional regulators like the New York State Department of Financial Services (NYDFS) introduced more strict cybersecurity rules that emphasize disclosure requirements. The SEC, in particular, took on a strong enforcement stance for public and private companies and has demonstrated this with fraud charges against individual CISOs.

In short: CISOs are having to do more with less and risk legal exposure, professionally.

In this rapidly evolving landscape, traditional CISO role characteristics may no longer suffice. This situation gives CISOs an unprecedented opportunity to argue for a place in the executive ranks.

Furthermore, the increased security pressure on organizations gives CISOs more ammunition to influence leaders outside of their direct sphere of control.

The 4th annual CISO Compensation and Budget study

The fourth annual CISO Compensation and Budget survey from IANS and Artico Search captured signs of unease and exposed opportunities for change.

Between April and October 2023, we collected data from 663 CISOs regarding their background, job level, compensation, budget dynamics, board engagement and job satisfaction. Additionally, between October and December 2023, we conducted unstructured interviews with approximately 100 CISOs to understand the challenges they face and their opportunities ahead. These CISOs represent a range of industries and company types across the U.S. and Canada.

This report presents the main findings with respect to the current state of CISOs. For added context, it includes perspectives from prominent security leaders and from executives at Artico Search, in particular Matt Comyns, co-founder and president, and Steve Martano, who is a partner in Artico Search's cyber practice and a member of the IANS Faculty of industry experts.

© 2024 IANS, Artico Search. All rights reserved. • 617.399.8100 • www.iansresearch.com

Fast-evolving expectations create opportunities for CISOs to level-up their position

The new SEC cyber rules and landmark cases that the agency brought against CISOs point to new legal and liability exposure. Regulators and prosecutors are now holding CISOs accountable for transparency, even fraud, on behalf of their organization. The situation has arisen in which the CISO is responsible for reporting requirements, similar to that of a chief financial officer, but often without the signature authority and general influence of a CFO.

Essentially, the expectations for the CISO role have been elevated to the C-suite level. Yet, we find many CISOs continue to struggle to be viewed as such and/or have not been elevated to that level.

FIGURE 1 highlights the contrasts between the new expectations and the reality on the ground, as reported by CISOs who took our survey.

FIGURE 1

Evolving Expectations Call for Changes in the CISO Role

New expectations resulting from the evolving cyber landscape and SEC rule changes vs. the current situation

The new expectations: **Arising from SEC rules and CISO accountability**	The current situation: **As reported by 660+ CISOs in the annual Comp and Budget survey**
The CISO to primarily serve as a **business risk function**, prioritizing business acumen over purely technical skills.	76% of CISOs come from a **mostly technical background**, where risk management is often secondary.
The CISO role as a **C-level position**, capable of bringing a clear voice into executive leadership meetings.	In 63% of cases, the **CISO role is a VP- or director-level position**. Just 20% of CISOs, and 15% of $1B+ company CISOs, are at the C-level.
CISOs have a **direct line of communication** with the CEO, C-suite and board, as well as the support of their leadership to get the resources they need.	90% of CISOs are at least two organizational levels removed from the CEO and just **50% of CISOs engage with their board quarterly**.

Most CISOs are considering a job change

Compared with 2022, CISO job satisfaction fell—a sign of unease with the status quo. The drop in satisfaction coincides with a growing share of CISOs considering a job change from 67% to 75%—an indication that most CISOs are seeking an improvement in job conditions.

This data suggests job dissatisfaction increases the likelihood of a CISO considering a career move. In contrast, CISOs who report high job satisfaction for key job aspects like their visibility with executives, career development, budget and compensation are generally less interested in a job change.

© 2024 IANS, Artico Search. All rights reserved. • 617.399.8100 • www.iansresearch.com

Why CISOs Should Read This Report

This report provides insights into the current state of the CISO. It uses data and analysis that can help CISOs understand their own situation and prepare arguments for driving change inside their own organization, including:

CISO role characteristics
These include title level, background and compensation. They lay bare opportunities or change, given the new expectations for CISOs.

CISO-board engagement
The frequency of engagement by company size and title level, as well as CISO expectations for guidance from their board.

CISO leadership skill development
The ways in which CISOs strengthen their soft skills to be able to bring a strong voice to executive leadership meetings.

CISO job satisfaction levels
Changes in satisfaction levels over the last four years that coincide with the challenges and opportunities that CISOs face.

Expert perspectives on the data
These come from prominent CISOs and executives at Artico Search based on their 15-plus years of CISO recruiting and career guidance.

This report is part of the Compensation, Budget and Org report series that also includes the 2023 Security Budget Benchmark Report, the 2023 CISO Compensation Benchmark Report, the 2023 Security Organization and Compensation Study, the 2023–2024 Security Staff and Career Report (coming soon), among others.

© 2024 IANS, Artico Search. All rights reserved. For more information, write to info@iansresearch.com.

Key Characteristics of the CISO Role at the Outset of 2024

This section looks at the key characteristics of the CISO function today, using data from 663 CISOs, in terms of scope of responsibilities, to whom they report, where they work and their background, among others.

Many CISOs are C-level in title, but not in organizational leveling

In the survey, we asked CISOs to select their job level, ranging from director to VP; executive (consisting of SVP and executive VP, or EVP); and up to the C-level, which is on par with the CFO and other C-suite executives. This section uses self-reported title-level data, irrespective of the respondents' reporting lines.

Each of the respondents indicated they are the highest-ranking professionals in the security organization. However, just 20% reported they are at the C-level on the overall organizational hierarchy.

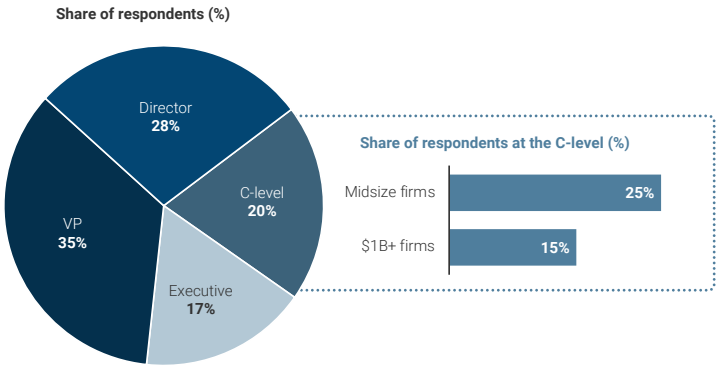
Among the CISOs who work at $1 billion-plus size organizations, based on annual revenue, 15% indicate they are at the C-level, versus 25% of CISOs at organizations with less than $1 billion in revenue, referred to as midsize firms (see FIGURE 2).

There being C-level CISOs at small or midsize companies does not necessarily indicate organizational maturity with regards to the cybersecurity function.

FIGURE 2

Most CISOs Are Not at the C-Level

Role level (%)



"Executive" constitutes SVP and EVP

Steve Martano explains:

At smaller companies, the organizational layers haven't been built because the company scale has not required it. In these cases, the head of security will probably report to a CEO or chief operating officer (COO); though, this usually changes with time as revenue and org design advance. What we typically see is that as these companies grow, they build out their organization and the CISO moves farther away from the C-level.

© 2024 IANS, Artico Search. All rights reserved. • 617.399.8100 • www.iansresearch.com

FIGURE 3 shows the breakdown of CISOs by organizational level across companies of various sizes by annual revenue.

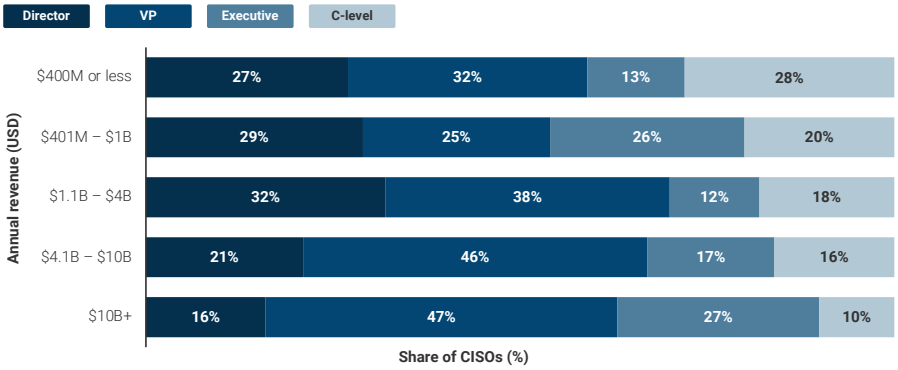
At firms with annual revenue exceeding $1 billion, CISOs are most likely in a VP-level position. At $10 billion-plus firms, 10% are C-level roles and 27% are at the executive level.

The chart also shows that the share of CISOs who are at the C-level increases as company size decreases, as Steve Martano explained earlier in this section of the report.

FIGURE 3

Most CISOs Are at the VP or Director Level

The organizational level of the CISO position (%)



Tech skills dominate CISOs' formative years

In the years leading up to the top job, the most common domains are IT/IT infrastructure, network security, security A&E and GRC.

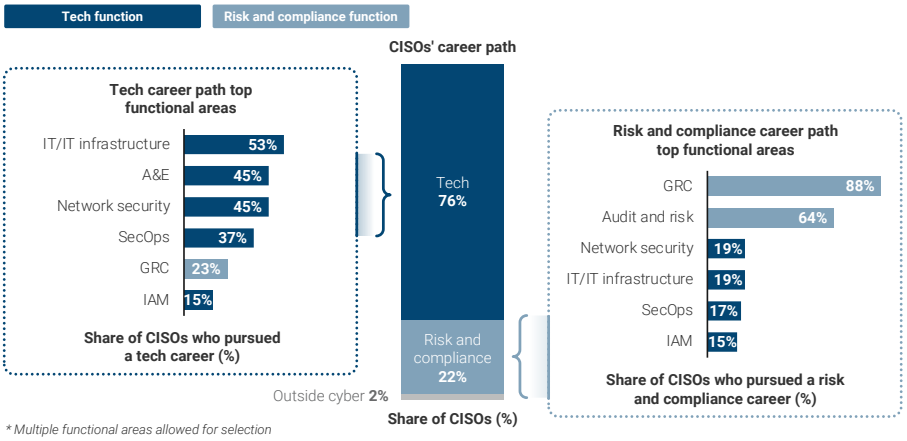
The two dominant career paths are a technical path and a risk and compliance path; although, some CISOs have crossed over during their formative years.

Just 2% of CISOs list domains outside cyber as key during their formative years (see FIGURE 4).

FIGURE 4

Most CISOs Pursued a Tech Career Path With a Minor Risk Focus

The top functional areas in CISOs' formative security years, prior to becoming a CISO*



** Multiple functional areas allowed for selection*

© 2024 IANS, Artico Search. All rights reserved. • 617.399.8100 • www.iansresearch.com

Traditional reporting lines prevail

A third of CISOs report into a business function, such as a CEO, COO, CFO or legal counsel. The remainder has a direct manager in a tech function, typically the CIO or chief technical officer (CTO).

These percentages have held steady from 2022 (see FIGURE 5).

The CISO at Amazon publicly advocates for a reporting line to the CEO, saying, "One of the reasons that Amazon is as good as we are at security is because security reports to the CEO and reports to the board regularly."[1]

Matt Comyns sheds further light on advantages and disadvantages of reporting to the CEO:

In some cases, CISOs reporting to a CEO works well, but in many cases, competing for the CEO's time can be limiting. At Amazon, the CISO reports to the CEO and they have a strong rapport. In other cases, a dotted reporting line to the CEO works better, as the CEO likely does not have time to get into the operational details of a security program but needs high-level security updates to stay informed of any serious risks or incidents.

FIGURE 5

A Third of CISOs Report Into a Business Function

Who is your solid-line manager?

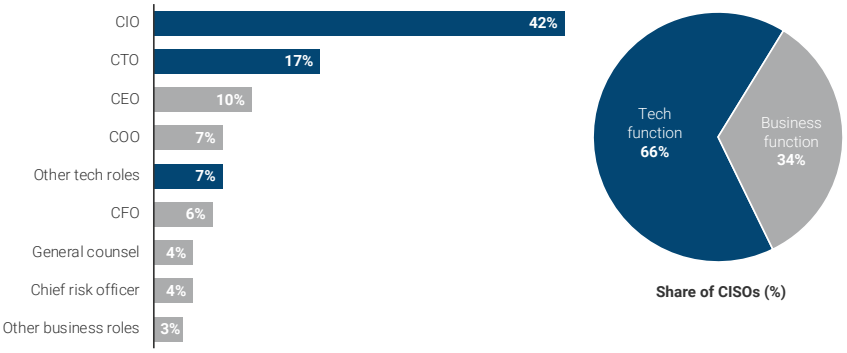
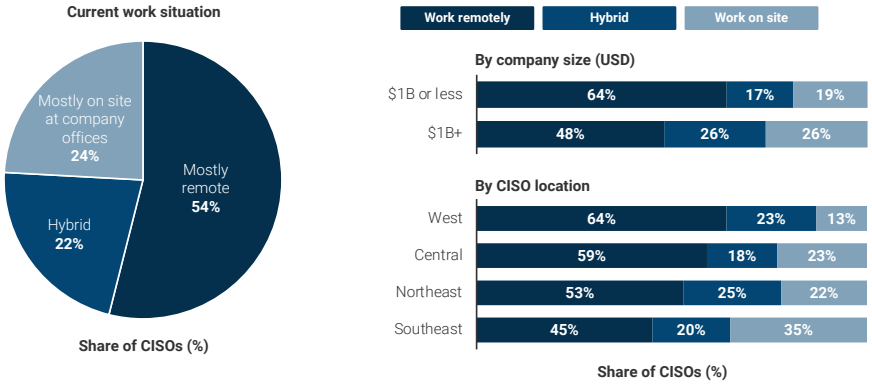


FIGURE 6

Roughly Half of CISOs Are Remote Workers, While 24% Work Mostly on Site

CISOs' current work situation



54% of CISOs work remotely

Similar to last year, 54% of respondents work mostly from their home office, 22% are in a hybrid situation and 24% generally work on site at their company offices. However, we see clear differences by company size and U.S. geographies.

For example, at organizations with revenues up to $1 billion, 64% work remotely, 17% are hybrid workers and 19% work mostly on site. For firms with revenues exceeding $1 billion, 48% work remotely, 26% are hybrid workers and 26% work on site.

In the West region, nearly two-thirds of CISOs are remote workers versus 53% in the Northeast and 45% in the Southeast (see FIGURE 6).

Matt Comyns explains what is behind the regional differences:

While West Coast-based firms—specifically, those in the Bay Area—tended to previously only recruit locally and have a strong in-office culture, more companies are abandoning expensive real estate in favor of a hybrid approach to work. It's a fairly new concept, so it's not surprising to see tech companies embracing it before other sectors and geographies.

1 Lila MacLellan. "Amazon's Chief Security Officer Says These Are the 6 Questions Every Board Should Ask Its CISO." Fortune. Oct. 24, 2023. https://finance.yahoo.com/news/amazon-chief-security-officer-says-114500674.html

© 2024 IANS, Artico Search. All rights reserved. • 617.399.8100 • www.iansresearch.com

The Importance of Recurring CISO Board Access

Having looked at the key characteristics of the CISO role in terms of types, experience, compensation, level, background and work location, this section transitions to the CISO relationship with the board of directors.

The updated SEC cyber rules and increased exposure that CISOs face call for strong collaboration between the CISO and company leadership, including the board. Our analysis of the survey data found there is a disconnect at most companies.

Half of CISOs engage with their board at least quarterly

The new expectations for CISOs flowing from the new SEC rules and CISO accountability advocate for regular and recurring CISO-board collaboration—quarterly updates, tabletop exercises and just generally gaining more of a rapport.

For half of the respondents, this is the case at their organization. They engage with their board quarterly—even more often when needed.

However, for 25%, board access is limited to just once or twice per year, 12% meets with the board purely on an ad hoc basis and 13% have no board engagement at all.

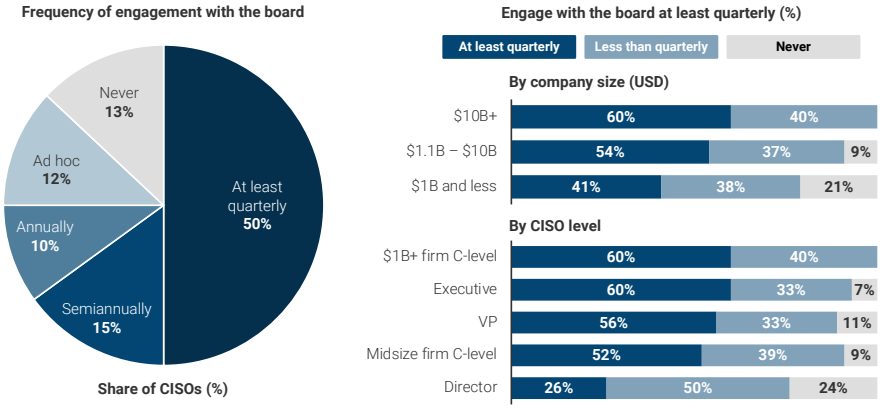
Even among companies with annual revenue exceeding $10 billion—most of which are publicly listed firms—just 60% of CISOs meet with the board regularly and 40% just once or twice a year.

Director-level CISOs are the least likely to have quarterly recurring board engagement (see FIGURE 7).

FIGURE 7

50% Of CISOs Engage With Their Board at Least 4 Times per Year

Share of CISOs (%)



© 2024 IANS, Artico Search. All rights reserved. • 617.399.8100 • www.iansresearch.com

CISOs with board access are more optimistic about budget and risk alignment

CISO satisfaction with the leadership's handling of security budget requests drops dramatically in absence of regular and recurring board engagement. Just 28% of those without board engagement are satisfied versus 57% with, at least, infrequent or ad hoc board contact.

The picture is similar for the share of CISOs who agree that the company risk profile and the security mandate are in alignment—a necessity in the face of legal exposure (see FIGURE 8).

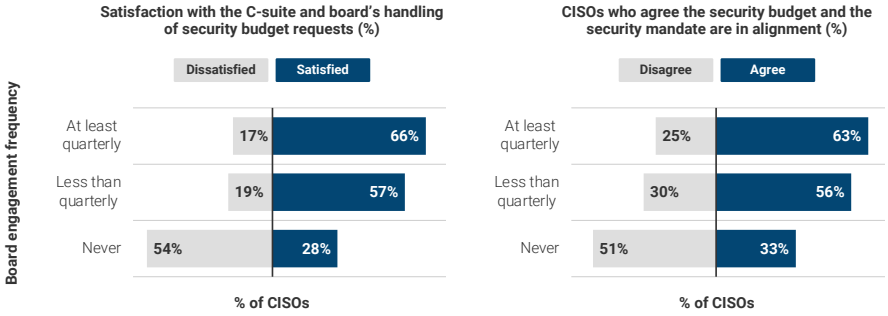
Steve Martano elaborates on this trend:

> *We see CISO satisfaction positively correlated with access and influence at the board level. CISOs with a strong rapport with their boards feel more valued and, generally, report they are 'heard,' even when there are disagreements on budgeting.*

FIGURE 8

Regular CISO-Board Engagement Boosts Internal Alignment on Budgets and Risk

Board engagement frequency, and the impact on handling of budget requests and internal risk alignment



Percentages do not add up to 100% because "neutral" responses have been excluded from the chart.

> *CISOs who manage relationships are more satisfied and successful than CISOs who manage technology. This also applies to the board. Regular engagement helps cultivate a deeper understanding of security's mandate among board members and strengthens alignment between the CISO and the organization's goals.*
>
> ***— Wolfgang Goerlich, advisory CISO and IANS Faculty***

CISOs seek clear risk guidance from boards, but often don't find it

Managing corporate risk is not just the business and operational responsibility of a company's management team—it is a governance and strategic issue that is squarely within the oversight responsibility of the board.[2]

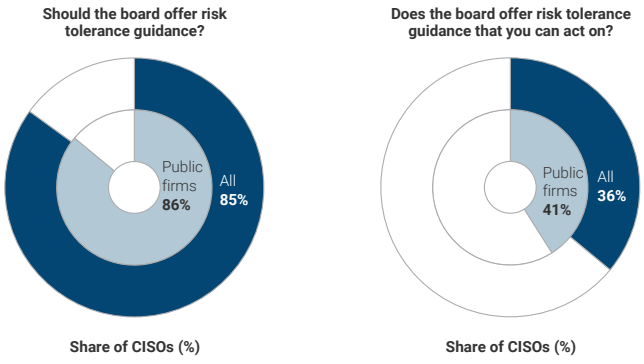
Eighty-five percent of CISOs in the survey indicated they believe their board should offer clear guidance on their organization's risk tolerance for the CISO to act on. However, just 36% find that this is indeed the case.

Even at publicly listed companies, just 41% of CISOs agree their board provides them with clear risk tolerance guidance (see FIGURE 9).

FIGURE 9

A Board's Risk Tolerance Guidance Often Fails To Reach the CISO

CISOs' expectations for their board on risk tolerance guidance



2 Martin Lipton, John Savarese, Sarah K. Eddy, Wachtell Lipton. "Risk Management and the Board of Directors." Harvard Law School Forum on Corporate Governance. Sept. 30, 2023. https://corpgov.law.harvard.edu/2023/09/30/risk-management-and-the-board-of-directors-9

© 2024 IANS, Artico Search. All rights reserved. • 617.399.8100 • www.iansresearch.com

A Seat at the Table Calls for New Skills

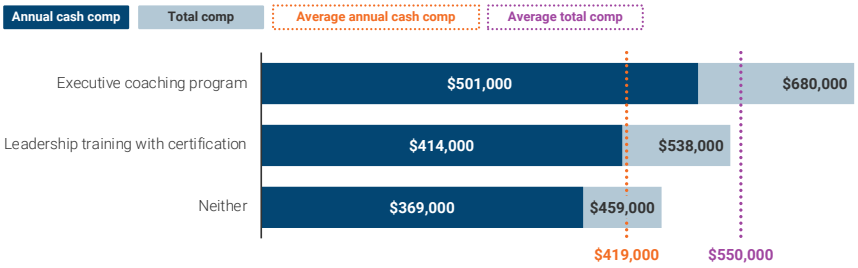
CISOs need to be able to communicate effectively with their board in order to meet reporting requirements, improve budget alignment and push for clear risk tolerance guidance. For that, they need:

- **Business acumen:** This comprises the skills that allow CISOs to speak the board's language, including a solid understanding of the corporate strategy and go-to-market; the financial literacy to read and comprehend financial statements; and the ability to frame risks in terms of economic impact and opportunity costs, instead of limited to technical vulnerabilities.
- **Executive presence:** The ability to be persuasive, direct and decisive in interactions with the board and C-suite and hinges on skills like storytelling, situational awareness and understanding the roles and responsibilities of the members of the board.

FIGURE 10

Compensation Is Higher for CISOs With Executive Coaching

Calculated annual cash compensation (base salary and target bonus) and annual total compensation (base salary, target bonus and equity) in USD



Most CISOs build out their leadership skills through coaching and external training

Formal leadership training courses and one-on-one executive coaching programs are effective tools for building business acumen and executive presence skills.[3]

Two-thirds of CISOs have completed, or are in the process of strengthening, their leadership skills through such programs.

CISOs who participate in, or have previously completed, such programs have higher pay. Some CISOs reach higher levels in the organization after completion of a leadership course and see their pay rise. Others are higher up, with higher pay, and then get invited to a training or coaching program.

Regardless of the sequence, the impact is significant, with the total comp of CISOs who are currently in or who have completed an executive coaching program exceeding those who haven't done a leadership skill development program by more than $200,000 (see FIGURE 10).

3 For more information, please see IANS Executive Competencies Program.

© 2024 IANS, Artico Search. All rights reserved. • 617.399.8100 • www.iansresearch.com

CISO Satisfaction Dips

This year's satisfaction ratings, which are a part of the survey data, suggest heightened anxiety among CISOs. Moreover, the data indicates a growing number of CISOs who are interested in a job change relative to prior years.

This section of the report provides key satisfaction trends.

CISO job satisfaction declines as consideration of job change rises

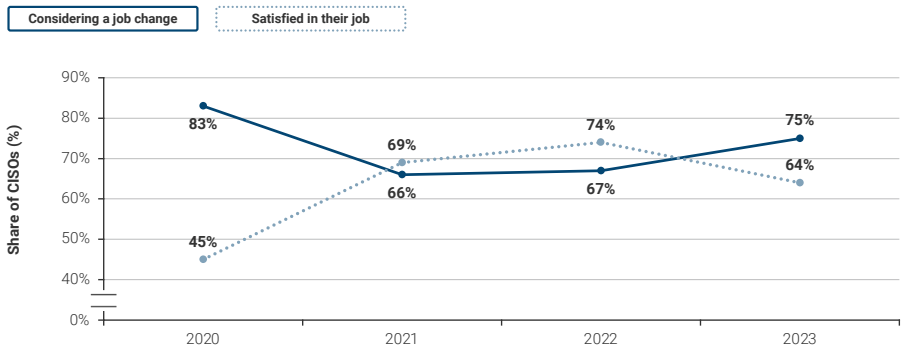
As expected, over a multiyear period, a change in CISO satisfaction is accompanied by an inverse change in the percentage of CISOs considering a job change.

Between 2022 and 2023, the share of CISOs who are satisfied in their job and company fell by 10 points to 64%. Meanwhile, the share that is open to a job change increased by 8 points to 75% (see FIGURE 11).

FIGURE 11

CISO Satisfaction Drops as Job Change Considerations Rise

Share of CISOs who are considering a job change in the next 12 months (%)



© 2024 IANS, Artico Search. All rights reserved. • 617.399.8100 • www.iansresearch.com

Methodology

IANS and Artico Search fielded the fourth annual CISO Compensation and Budget survey in April 2023. From early April until the end of October, we received survey responses from 663 security executives from companies that varied by size, location and industry.

We also conducted unstructured interviews with approximately 100 CISOs throughout October and November in 2023.

Key steps in the research process are:

Survey design
We improve our surveys on an ongoing basis by incorporating feedback from respondents and adding topics based on client demand.

Respondent recruitment
We recruit from last year's already-vetted respondents. We grew the sample by recruiting from diverse CISO audiences.

Data hygiene
The survey design and data collection process include precautions to prevent fake responses and survey response errors. For example, respondents can skip questions if they don't have access to the requested information.

Analysis
A five-member team runs the analysis, builds the storyline and writes the report. This is a multidisciplinary team with combined expertise in data science, cybersecurity, CISOs' key imperatives, and cyber executive talent and recruitment.

Objectivity
This research is neither influenced by nor paid for by third parties. We report on the data objectively and free from personal bias and opinions. Clarifying insights are drawn from Artico Search's cyber practice and clearly marked as quotes.

Sample breakdown

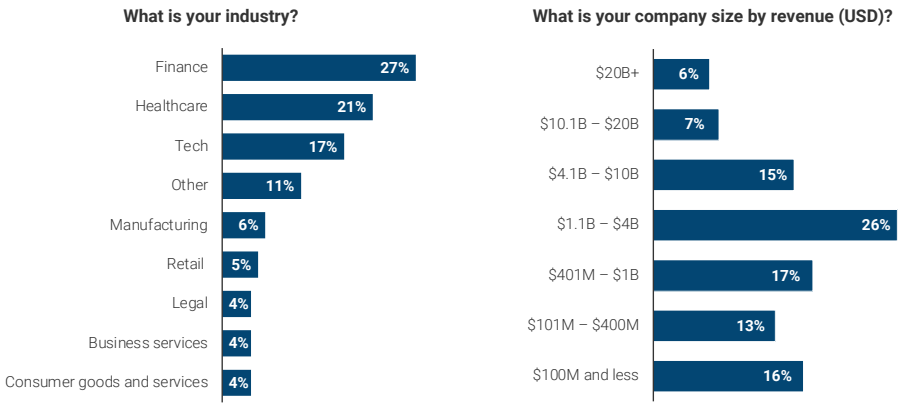
Of the sample of 663 CISOs, 609 work in the U.S. and Canada.

The three largest industries in terms of representation among CISOs in the U.S. and in Canada in the sample are finance (27%), healthcare (21%) and tech (17%).

Nearly half (46%) of respondents work at companies with less than $1 billion in annual revenues, 41% work at firms with $1 billion to $10 billion in annual revenue, and 13% represent companies with more than $10 billion in annual revenue (see FIGURE 12).

FIGURE 12

Breakdown of the Survey Respondents by Company Type



The "Other" category includes mainly education, transportation, government and utilities

Respondents provided their compensation metrics, including base compensation, target bonus percentage and equity percentage. These three metrics allowed us to compute the annual cash compensation (base salary plus bonus) and total annual compensation (cash compensation plus equity) for each respondent. We then calculated the averages across the relevant sample. These are provided in several places in the report.

© 2024 IANS, Artico Search. All rights reserved. • 617.399.8100 • www.iansresearch.com

About Us

This publication is created in partnership between IANS and Artico Search.

Artico Search

articosearch.com

Founded in 2021, Artico Search's team of executive recruiters focuses on a "grow and protect" model, recruiting senior go-to-market and security executives in growth venture, private equity and public companies. Artico's dedicated security practice delivers CISOs and other senior-level information security professionals for a diverse set of clients.

IANS

iansresearch.com

For the security practitioner caught between rapidly evolving threats and demanding executives, IANS is a trusted resource to help CISOs and their teams make decisions and articulate risk. IANS provides experience-based insights from a network of seasoned practitioners through Ask-an-Expert inquiries, a peer community, deployment-focused reports, tools and templates, and executive development and consulting.

© 2024 IANS, Artico Search. All rights reserved. • 617.399.8100 • www.iansresearch.com