IANS + ARTICO

2025 The State of the CISO

Summary Report

This summary report provides high-level insights from our 2025 State of the CISO Report.

The complete State of the CISO Report is a comprehensive, 28-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.

Table of Contents

Executive Summary 4

As CISOs' scope expands, new career opportunities emerge

CISO Positioning Within Their Organizations 5

CISOs in the organizational hierarchy

How often CISOs engage with their boards

The analysis found 3 CISO segments

Satisfaction differences among segments

Strategies to build access and influence

Emerging Career Advancement Opportunities 11

How broader scope impacts compensation

Higher pay for CISOs with dual security and IT responsibilities

New career opportunities for CISOs

Methodology 16

Sample breakdown

About Us 18

Artico Search

IANS

Executive Summary

As the cybersecurity function becomes increasingly integral to organizations, the CISO role continues to grow in importance, complexity and scope of responsibilities. This evolution presents an opportunity for CISOs to expand their strategic influence with top leadership and opens up avenues for professional growth. By effectively navigating these changes, CISOs can elevate their impact and unlock new career paths—and, in many cases, achieve even greater job satisfaction and higher compensation.

This report describes the changes to the CISO role in detail and offers recommendations for CISOs navigating the challenges associated with this evolution. It provides analysis of our fifth annual CISO Compensation and Budget Survey, which drew responses from more than 800 CISOs across diverse industries, company sizes and organizational types.[1] We offer insights into the current state of the CISO profession and the changes taking place in terms of remit and expectations. We also detail the sectors and companies that are leading in this transition.

This report is produced jointly by IANS and Artico Search. Data scientists and researchers from IANS collect data, run analyses and engage with CISOs to identify trends and market insights. Market experts at Artico Search, including Steve Martano, IANS Faculty member and partner in Artico Search's cyber practice, and Matt Comyns, Artico Search's co-founder and president, provide actionable guidance and relevant quotes, helping CISOs to navigate this pivotal time.

As CISOs' scope expands, new career opportunities emerge

Most CISOs are experiencing a growing scope of responsibilities, expanding into areas beyond information security, such as business risk, broader security functions, IT and digital transformation. This evolution can be challenging to manage and does not always lead to greater satisfaction with career development. However, when managed effectively, expanded scope can lead to greater executive-level access and visibility, opening new opportunities for career advancement—a welcome prospect for tenured CISOs at large public enterprises who have been asking themselves, "What's next?"

Newly emerging roles in billion-dollar enterprises include the dual CISO/CIO position, with full responsibility over security and IT, effectively reversing the traditional model of IT overseeing security. Other executive-level opportunities include the chief risk officer (CRO) role, managing enterprise-wide risk and processes, or the emerging chief trust officer role, especially in industries such as financial services or tech, where trust and transparency are critical to business operations and customer relationships. Additionally, some CISOs take on board seats at publicly traded companies, providing essential cybersecurity expertise.

1 All survey respondents are the senior-most leaders in their respective cybersecurity organizations. While most hold the CISO title, exact titles may vary. For simplicity and readability, we refer to this group collectively as "CISOs".

CISO Positioning Within Their Organizations

CISOs often cite executive-level access as a critical ingredient to driving organizational impact and enhancing their effectiveness. Executive-level access enables active participation in strategic business discussions and decision-making, allowing CISOs to discuss security risks with top leadership and align security strategies with overarching business objectives.

A CISO's reporting structure plays a significant role in shaping their visibility and influence. CISOs who are part of, or have direct lines to, the C-suite are more likely to participate in strategic conversations compared to peers positioned several layers below the CEO. Similarly, building a trust-based relationship with board members starts with having regular opportunities to engage with them.

This section explores where CISOs fit within organizational hierarchies and the extent to which CISOs engage with their boards.

CISOs in the organizational hierarchy

Approximately 39% of CISOs hold executive-level titles, including EVP and SVP, which is a gradual increase from 35% two years ago. Among these executive-level CISOs, 35% at smaller organizations (with annual revenues up to $1 billion) report directly to the CEO, compared to 12% at larger enterprises (with revenues exceeding $1 billion). In contrast, just 3% of large-firm director-level CISOs report to the CEO, with more than a third separated from top executives by at least three organizational layers (see FIGURE 1 on the next page).

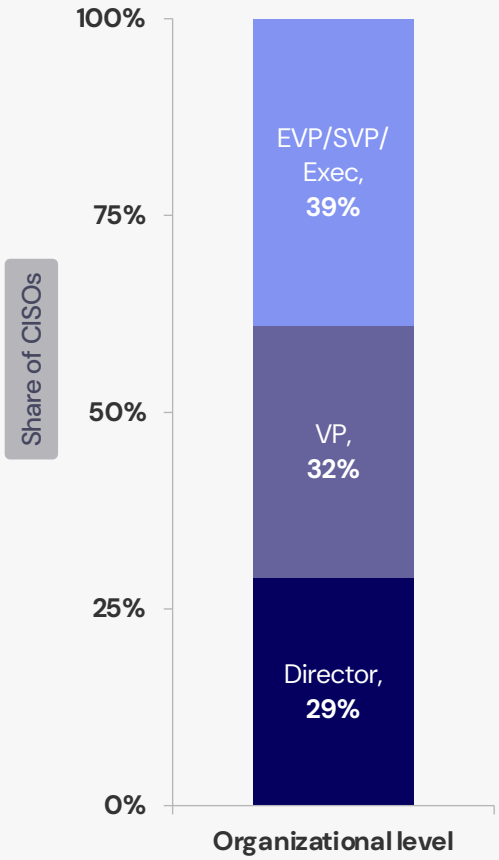
These disparities underscore significant differences in strategic influence and organizational alignment between director- and executive-level CISOs.

FIGURE 1 *Source: IANS & Artico Search*

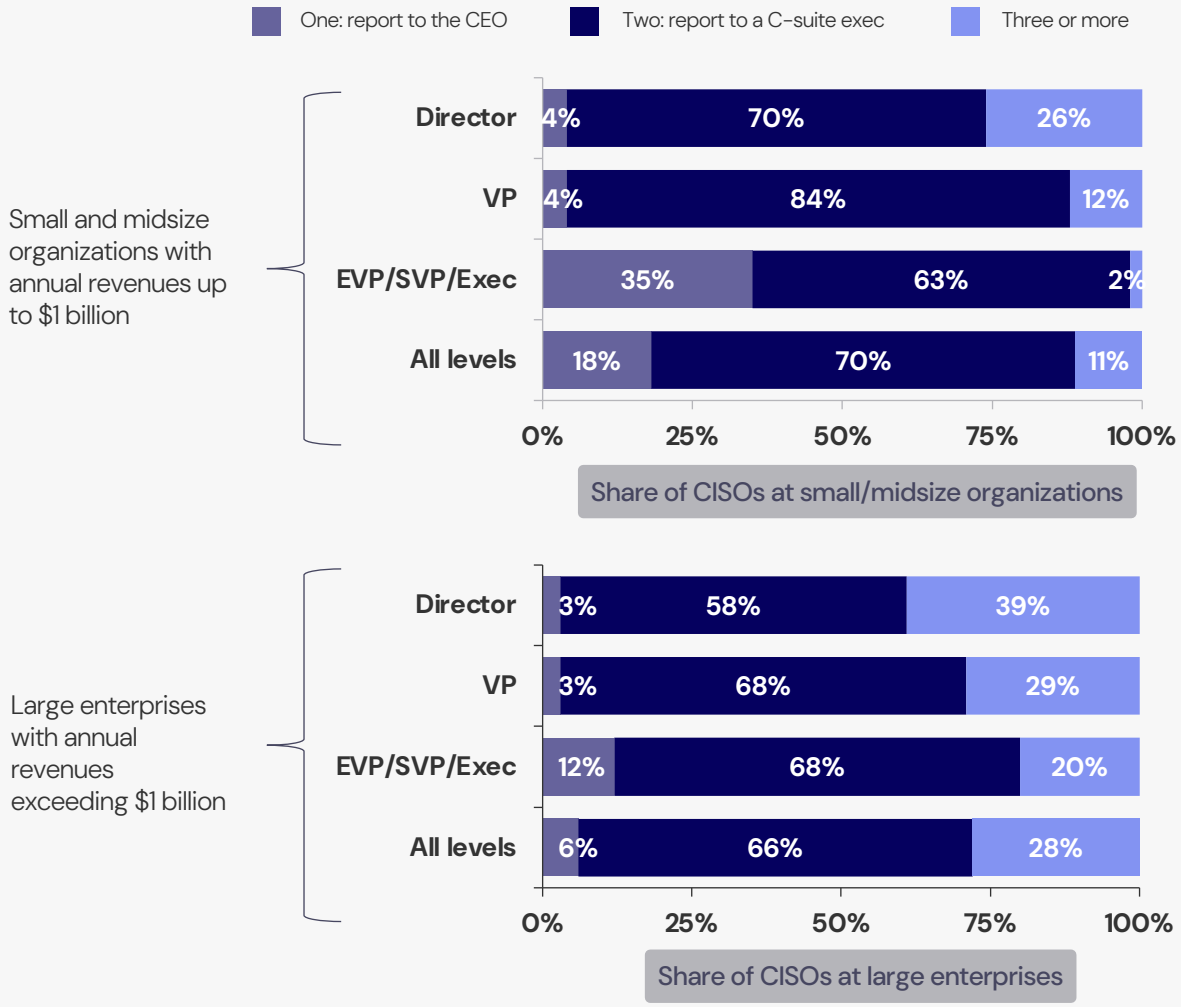
Most CISOs Are VP Level or Higher, With Close Proximity to the C-Suite

The organizational level of the CISO and organizational layers removed from the CEO

At what organizational level is your role?



How many layers are you removed from the CEO?



How often CISOs engage with their boards

Currently, 47% of CISOs engage with their boards monthly or quarterly. In enterprises with annual revenues exceeding $10 billion, 65% of CISOs have at least quarterly board engagement. In contrast, smaller organizations with annual revenues under $400 million lag behind, with 37% having monthly/quarterly board engagement and 42% meeting with their boards on an ad hoc basis, if at all (see FIGURE 2).

It is clearly more common for CISOs to have board visibility and influence at larger organizations with more-developed risk governance structures and a responsibility to adhere to regulations that require boards to oversee cybersecurity risks. CISOs at smaller, often privately held firms may need to create other opportunities to engage with board members if they don't engage as often during formal meetings.

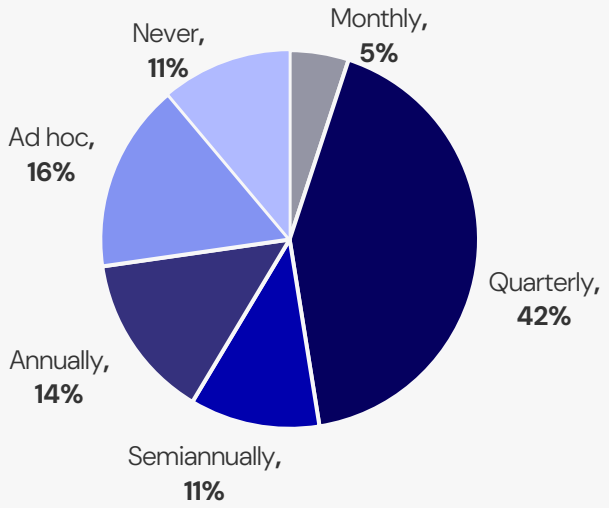
> In today's environment, the alignment of cyber governance and cyber operational programing is critical to a successful program. Enterprise CISOs at large, publicly listed companies should strive to develop relationships with board members outside of formal quarterly board meetings. Whether it's reporting to a committee, serving on a committee, ad hoc one-on-one meetings, etc., CISOs should utilize the macro environment and focus on security to continue developing a rapport with their company's board members.
>
> *Steve Martano*

FIGURE 2 *Source: IANS & Artico Search*

Half of CISOs Report Quarterly or Monthly Board Engagement, Rising to Two-Thirds at $10B+ Firms

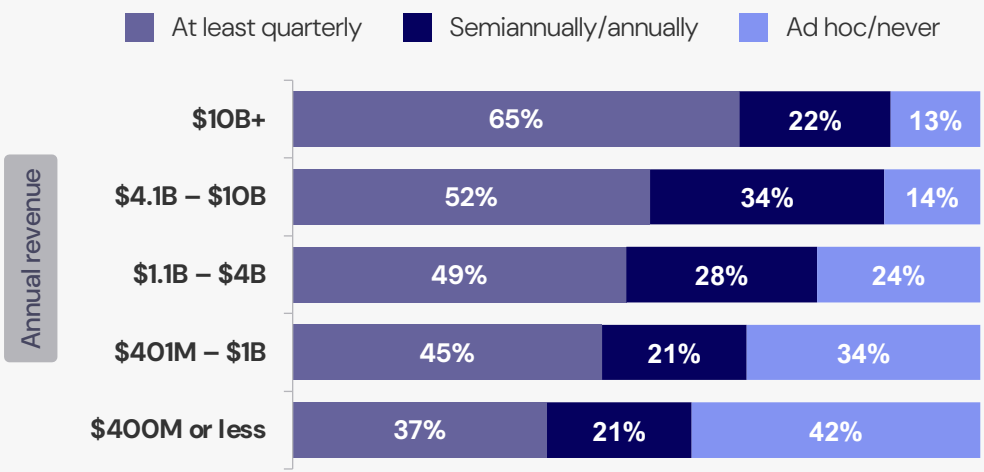
How often do you engage with the board of directors?

How often do you engage with the board of directors?



Share of CISOs

CISO-board engagement frequency, by company size



Share of CISOs

The analysis found 3 CISO segments

As shown, companies are at different stages in terms of giving their CISO greater C-level access and boardroom influence. C-level access is associated with holding an executive-level position with close organizational proximity to the CEO, and boardroom influence is tied to monthly or quarterly engagement with the full board or serving as a board subcommittee member.

By evaluating respondents along these two dimensions, we identified three distinct segments:

Strategic CISOs (28%): These CISOs report directly to the CEO or occupy a high-ranking position in the hierarchy and, therefore, hold significant influence within their organization and with top executives. They maintain regular engagement with the board, meeting at least quarterly, either in full board sessions or as members of subcommittees—facilitating mutual understanding and aligning on strategic priorities between the CISO and top leadership.

Functional CISOs (50%): This group excels in one of the aforementioned areas—either C-suite access or boardroom influence—but lags in the other compared to peers in the Strategic group.

Tactical CISOs (22%): These CISOs have limited executive-level access due to their lower organizational rank and sporadic board engagement.

Having identified these three segments, we looked at the types of industries and companies where these CISOs are commonly found. Certain sectors appear more frequently within a segment, along with notable differences in company size, types and the experience levels of CISOs.

> CISOs who successfully navigate the complexities of the C-suite and the boardroom command higher salaries. These CISOs drive more visibility by adding value in business risk conversations and decisions, are viewed on-par with other peers in the C-suite, and are considered strategic business executives, rather than technology leaders.
>
> *Matt Comyns*

Satisfaction differences among segments

Besides compensation differences among segments, we also analyzed trends in job satisfaction. We focused on CISOs' self-reported satisfaction with two important elements:

- **Satisfaction with executive visibility:** The recognition and presence a leader has among top executives and decision-makers.
- **Satisfaction with career development:** The professional growth and progress of their careers, including support from their organization related to career development such as mentorships, training and networking opportunities.

The results show CISOs in the Strategic segment are twice as likely to report being "very satisfied" with their career development compared to those in the Tactical group. Satisfaction levels for the Functional segment fall in between those of the Strategic and Tactical groups (see FIGURE 5).

FIGURE 4 *Source: IANS & Artico Search*

The Strategic CISOs Group Leads in Compensation and Financial Upside Potential

Average annual cash compensation (base salary and target bonus) and total compensation (base salary, target bonus and equity) average, median and top ranges for U.S.-based CISOs, in USD

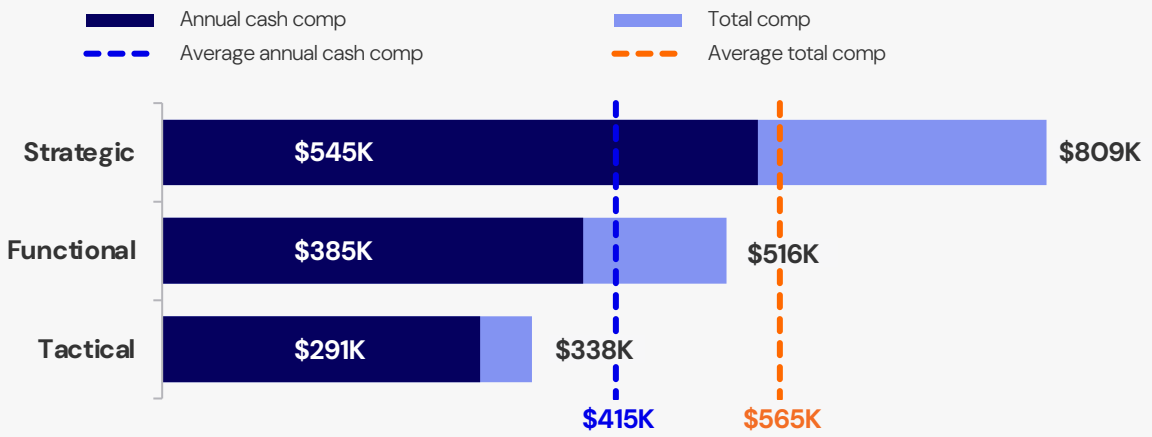
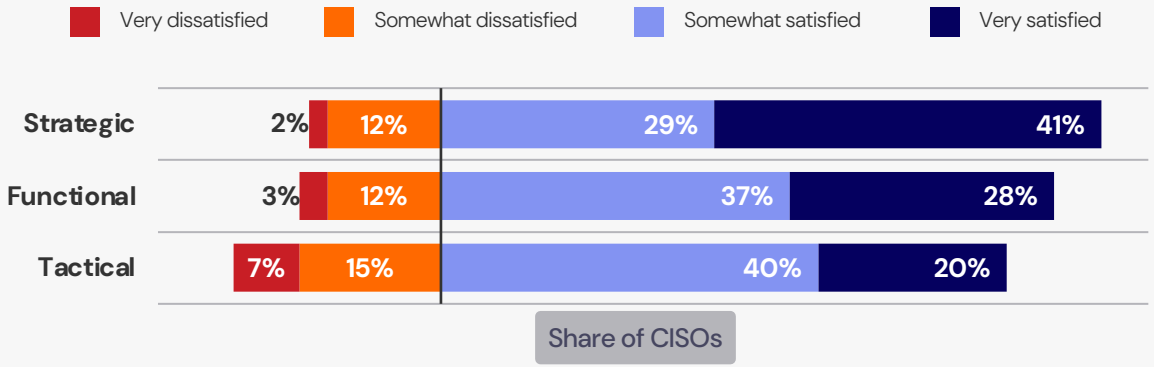


FIGURE 5 *Source: IANS & Artico Search*

CISOs in the Strategic Segment Report Higher Satisfaction

How satisfied are you with your career development?



Percentages do not add up to 100% because "neutral" responses are not included in the chart.

Strategies to build access and influence

The absence of adequate C-level access or opportunities to engage with the board can lead to frustration among CISOs and cause them to feel undervalued or constrained in their role. We see this reflected in the large share of CISOs within the Tactical segment that expresses dissatisfaction with their level of executive visibility. However, we also observe meaningful pockets of dissatisfaction among CISOs in the Strategic and Functional groups.

The concerns CISOs articulate vary depending on their segment, but there are some common themes. Drawing on insights from our experts at IANS and Artico Search, we provide actionable recommendations below to help CISOs overcome these barriers.

Strategic CISOs: "I have a seat at the table, but I'm not recognized as a true executive partner"

Even Strategic CISOs who are close to leadership and invited to critical board sessions may find themselves perceived more as technical operators who provide mandatory updates on security maturity models, rather than as thought partners with truly strategic input and impact, undermining their influence and limiting their effectiveness in driving business-wide initiatives.

Recommendations: Start by reflecting on your current brand within the organization. Are you seen as a technical leader or a strategic partner on par with the CFO, chief product officer, or chief revenue officer? If it is the former, cultivate relationships with key executives to shift that perception. Shift your approach from providing technical updates to initiating more open-ended, strategic governance discussions.

Functional CISOs: "I don't have time to be strategic"

Functional CISOs often find their time consumed by operational demands, leaving little room for strategic initiatives. Scope creep hinders their ability to focus on leadership and limits their career growth.

Recommendations: Delegation is key to freeing up your time for strategic work. Build and organize your team with clear roles and responsibilities, equipping your leaders to take ownership of operational tasks so you can focus on broader organizational priorities.

Tactical CISOs: "I'm not getting invited"

Tactical CISOs often struggle to secure time with top leadership and board members. Without this access, they miss critical opportunities to advocate for their security program and communicate security risks and priorities, potentially leaving the organization more vulnerable.

Recommendations: To overcome this, start by increasing your visibility within the organization at large. Volunteer for cross-functional projects and committees and help your colleagues understand how these initiatives are connected to security issues. This can include presenting case studies, industry trends or actionable solutions that align security priorities with organizational objectives. By engaging with leaders from a diverse range of disciplines, you can showcase your broader value and open pathways to higher-level conversations.

Emerging Career Advancement Opportunities

Besides gaining top-level access and influence, the scope of responsibilities associated with the CISO role continues to evolve. Our survey data over the past five years, combined with ongoing conversations with CISOs, confirms that the CISO role continues to expand into adjacent domains.

Figure 6, on the next page, shows the current distribution of CISO role scope reflected in our survey results, with:

Near-universal (90%+) responsibility over infosec domains, including security operations, architecture and engineering, and infosec GRC, as well as digital risk and compliance.

The majority (50% – 99%) has an expanded infosec scope that includes IAM, application security and/or cloud security. In addition, the majority have taken on more business risk functions such as business continuity and third-party risk management, as well as product security—a broader security area.

A significant portion (25% – 50%) oversees enterprise risk management and taking on broader security functions such as physical security, privacy or fraud protection, or has ownership over parts of the IT stack.

An emerging share (less than 25%) is broadening their scope to include emerging domains including AI, M&A security, data governance, comprehensive IT oversight, and even digital transformation and innovation. Because many of these responsibilities more directly impact corporate strategy and performance, they may allow CISOs to exert greater influence on the organization.

FIGURE 6 *Source: IANS & Artico Search*

The Scope of CISO Responsibilities Continues To Expand

What is included in your ownership?

FIGURE 6.1. The growing scope of CISO responsibilities

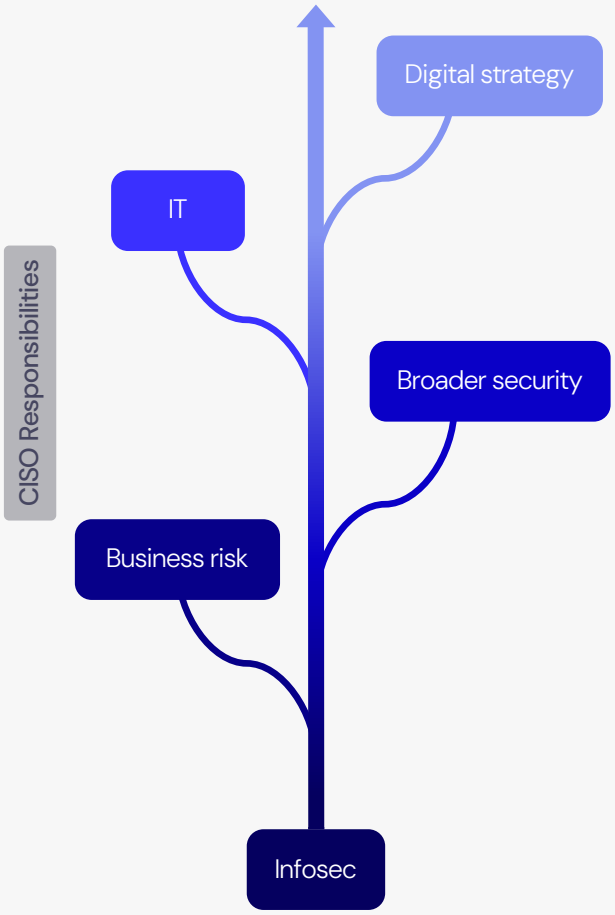


FIGURE 6.2. Areas within each domain and the percentage of CISOs overseeing them

	Share of CISOs with ownership			
	Universal 90%+	**Majority 50% – 90%**	**Significant 25% – 50%**	**Emerging 1% – 25%**
Digital strategy				• Digital transformation • Innovation
IT			• Parts of IT • OT	• All of IT • IT due diligence
Broader security		• Product security	• Physical security • Privacy • Fraud protection	• Data governance • Change management
Business risk	• Digital risk and compliance	• Business continuity • Disaster recovery • Third-party risk management	• Enterprise risk management	• AI • M&A security • Trust and safety
Infosec	• Security operations • Architecture/ engineering • Infosec GRC	• IAM • Application security • Cloud security		

How broader scope impacts compensation

As CISOs assume a broader scope of responsibilities, questions arise about how these changes influence compensation and whether job satisfaction differs for CISOs in expanded roles compared to those in more-traditional setups. This section addresses both.

We addressed the compensation question by analyzing survey data that asked CISOs about their wage growth, specifically the percentage increase in their compensation over the past 12 months and the primary driver of that change. The data shows wage increases associated with assuming additional responsibilities are rare, with only 3% of CISOs attributing their raises to taking on larger scope. For this group, the average wage growth was 13%.

Meanwhile, 7% of CISOs reported their comp increases were primarily driven by a change in employers—a move often accompanied by taking on a larger role with more responsibilities. This group experienced an average increase of 31%.

The majority of CISOs (70%) indicated their raises were annual merit increases, averaging 6%. Given that many of these CISOs have mentioned in conversations that their responsibilities have grown, this data suggests most are not explicitly (nor significantly) financially rewarded for the expansion of their scope.

> Not all increases in scope directly lead to an increase in compensation. Taking on added responsibilities, such as digital risk or physical security, aligns naturally with the digital evolution of security, enabling a CISO to drive more efficiency and influence in their organization. While this increase in responsibility may lead to greater operational efficiency, this scope is generally not tied to a significant increase in compensation. On the other hand, a promotion to chief security officer, or a dual CISO/CIO role or CISO/chief digital officer role, is generally associated with a compensation boost, as these domains redefine the role and its expectations in a meaningful way.
>
> *Steve Martano*

Higher pay for CISOs with dual security and IT responsibilities

The picture changes for CISOs who take on IT ownership. We compared the pay levels of three groups:

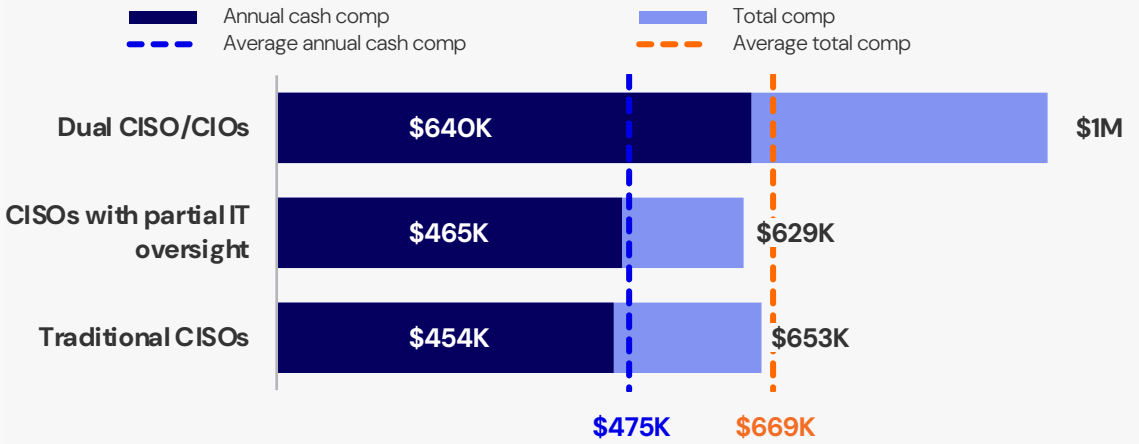
- **Dual CISO/CIOs:** These leaders head up security orgs where IT is fully integrated—overseeing security and all IT functions.
- **CISOs with partial IT oversight:** These CISOs oversee select IT areas, such as IT operations, networking and infrastructure, alongside security.
- **Traditional CISOs:** These leaders do not manage any IT functions but may oversee business risk and broader security functions in addition to their infosec responsibilities.

To ensure a fair analysis, we excluded small and midsize organizations, where security and IT are sometimes combined under a single executive for budgetary reasons. Instead, we focused exclusively on compensation differences among these groups at enterprises with annual revenues exceeding $1 billion.

FIGURE 8 *Source: IANS & Artico Search*

Dual CISO/CIOs at Large Enterprises Have Higher Compensation Than Traditional CISOs

Average annual cash compensation (base salary and target bonus) and total compensation (base salary, target bonus and equity) average, median and top ranges for U.S.-based CISOs, in USD



The analysis shows large organizations pay higher compensation to dual CISO/CIOs, with an average annual pay of $1 million and the top quartile starting at $1.5 million. In comparison, the cash and total compensation averages for CISOs with partial IT oversight and traditional CISOs are more closely aligned—except for the very top earners (see FIGURE 8).

This would seem to indicate taking on all of IT is highly rewarded, but being given some IT functions opportunistically—perhaps due to the departure of another IT executive or unclear lines of ownership between infosec and IT—is not a reliable path to higher compensation.

New career opportunities for CISOs

Resulting from greater scope, C-level access and board influence, new career opportunities are emerging for CISOs. The dual CISO/CIO position has emerged in 15% of organizations in our sample and represents 7% of CISOs at enterprises with annual revenues exceeding $1 billion.

Anecdotally, we observe CISOs transitioning into business-focused executive roles, such as CRO, using their experience managing enterprise-wide risks and processes. Similarly, the chief trust officer role is also gaining prominence as a potential career step for CISOs in product-driven organizations. This role emphasizes managing the trust relationship with customers, combining elements of security, privacy and customer experience.

Additionally, there is a niche trend of CISOs transitioning to external board positions, either as full board members or advisors, where they can provide critical cybersecurity governance expertise. However, there is limited appetite for most public boards to add a cyber expert at this time.[5]

These evolving career trajectories underscore the growing strategic importance of the CISO role and the valuable, multidisciplinary skill set these leaders bring to organizations. This evolution is in its early stages. CISOs thinking about their long-term career trajectory can benefit from careful reflection on the aspects of the job they are uniquely skilled at and work to take on relevant side projects that align with business imperatives. Becoming a trusted partner in these initiatives is often the natural steppingstone into emerging executive roles such as chief trust officer or chief digital risk officer.

> When thinking about expanded scope of responsibility, CISOs should consider how the additional scope is viewed by the organization and the market. The best added sets of responsibility for a CISO drive a more-efficient program and provide access to cross-functional stakeholders, allowing security leaders to work more closely with leaders outside of security and become increasingly embedded in business operations. CISOs can use added responsibilities to elevate their programs and their brands to become more marketable in the next role.
>
> *Steve Martano*

5 Read our analysis into CISOs' readiness to serve on public company boards in the 2023 report CISOs as Board Directors: CISO Board Readiness Analysis.

Methodology

IANS and Artico Search fielded their fifth annual CISO Compensation and Budget survey in April 2024. From April until November, we received survey responses from 830 security executives at a diverse set of companies with regard to size, location and industry. Of them, 757 U.S.- and Canada-based respondents completed the compensation section of the survey.

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. Respondents receive a complimentary copy of the research. There is no monetary compensation attached to taking the survey.

Data hygiene

The survey design and data collection process includes precautions to prevent fake respondents 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

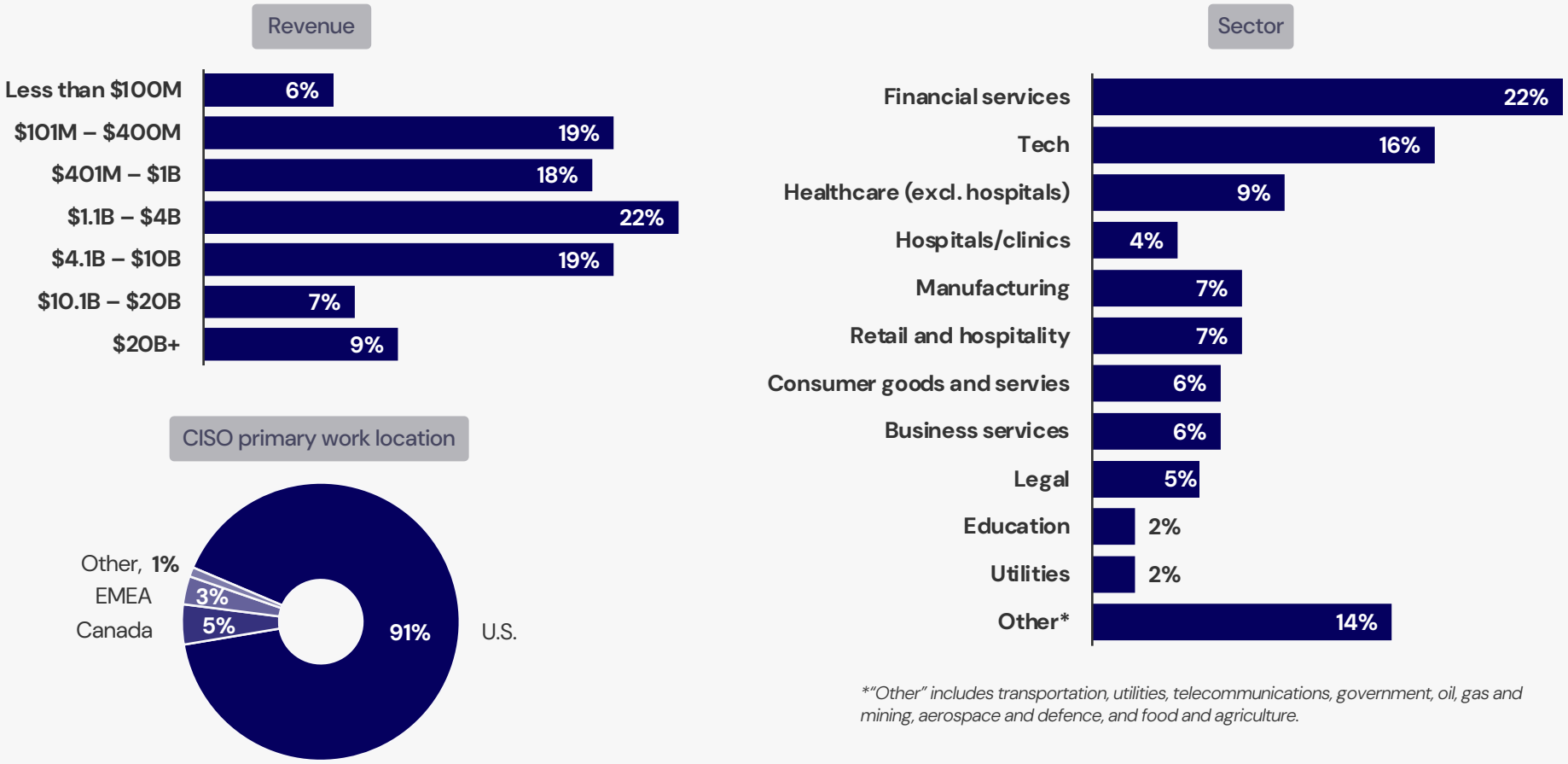
This research is neither influenced by nor paid for by third parties. We report on the data objectively and free from personal bias and opinions. Clarifying insights are drawn from Artico's cyber practice and clearly marked as quotes.

Sample breakdown

FIGURE 10 provides the breakdown of respondents by company industry, company size in revenue and primary CISO work location.

FIGURE 10 *Source: IANS & Artico Search*

Sample Breakdown: N = 830



**"Other" includes transportation, utilities, telecommunications, government, oil, gas and mining, aerospace and defence, and food and agriculture.*

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.