2025 Compensation and Budget for CISOs in Large Enterprises

Benchmark Summary Report

Table of Contents

This summary report provides high-level insights from our full 2025 Large Enterprise Report.

The complete 2025 Large Enterprise Report is a comprehensive 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.

IANS and Artico Search have recently published a series of reports for CISOs, covering key topics such as security budgets, compensation and the evolving role of the CISO. This latest report continues the series, with a specific focus on organizations with annual revenues exceeding $1 billion—a segment we refer to as "large enterprises."

Organizations in this segment are inherently complex due to their vast size; diverse business operations; and the sheer number of employees, stakeholders, data assets, access points and communication channels, which increase the challenges of managing risk, security and organizational cohesion. Additionally, their size alone makes them high-value targets for sophisticated threat actors. Compared to midmarket organizations, these larger-scale enterprises are generally better funded, allowing them to maintain extensive security programs.

This report provides insights into large enterprises' security programs. It offers CISOs data and perspectives on the budget and staffing levels at similarly scaled firms and compares their salary, span of control and experience level against that of their peers.

The findings are based on data from the 2024 annual CISO Compensation and Budget survey, conducted jointly by IANS and Artico Search. From April through December 2024, 862 CISOs from a wide range of industries and company sizes responded.[1] Of those, 406 work at large enterprises.

Recognizing the significant variation within this catagories, this report groups enterprises into four segments, based on annual revenue:

$1B – $2B
Comprising 20% of the sample, these companies are on the cusp of the large enterprise threshold. They are still maturing in terms of governance, security and scalability and often face unique challenges of transitioning to large-scale operations.

$2B – $5B
Making up 34% of the sample, these mid-tier firms generally have more-established governance structures, more-developed operations and manage more-extensive vendor ecosystems than those in the $1B – $2B segment.

$5B – $20B
Representing 31% of respondents, these operationally mature organizations generally have diversified business lines, complex organizational structures and multinational operations.

$20B+
Accounting for 15% of the sample, these Fortune 200-equivalent companies are highly complex, distributed organizations with security strategies that tend to address geopolitical risk, nation-state threats and critical infrastructure interdependence.

For additional insight, this report features expert perspectives from Artico Search executives, including Steve Martano, a member of the IANS Faculty and partner in Artico Search's cyber practice, and Matt Comyns, co-founder and president at Artico Search.

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

Executive Summary

This report provides a comprehensive snapshot of security programs and the characteristics of the CISO role at large enterprises. In general, as revenue increases, so, too, does the scope and complexity of security programs. Larger enterprises tend to have bigger security budgets; larger teams; more-experienced CISOs in higher-level positions with more-senior reporting lines; and higher compensation levels, particularly large-scale equity stakes that make up a considerable part of total annual compensation.

Highlights of the research presented in this report include:

Security budget and headcount metrics

In the large enterprise segment, security budgets range from the low single-digit millions to more than $100 million. Budget and staff size scale with revenue, with security budget as a percentage of revenue averaging about 0.35% (roughly $3.5 million per $1 billion in revenue).

CISO compensation

The average total compensation for large enterprise CISOs is $700,000 (including base salary plus bonus and annual equity). Compensation increases with company revenue, with CISOs at $20B+ enterprises averaging $1.1 million in total comp. This segment has the highest concentration of top 10% earners, reflecting the scale and complexity of managing large security budgets and teams, as well as the strategic relationship management skills required of these CISOs.

Organizational position of the CISO

Half of $20B+ firm CISOs are at the executive level (EVP, SVP or equivalent), reflecting strategic influence and direct access to top leadership. In the $2B – $5B and $5B – $20B segments, this figure is significantly lower (27% and 31%, respectively), with more CISOs at the VP or director level.

CISO board engagement

As board-level attention has increased in recent years, so has direct CISO engagement with boards. Currently, 53% of large enterprise CISOs regularly engage with the full board at least quarterly. This figure is even higher in the $5B – $20B and $20B+ segments, where complexity and regulatory scrutiny are greatest.

CISO background

Larger company size and complexity correlate with more-experienced CISOs. On average, large enterprise CISOs have 10 years of experience in the role, often across multiple employers and industry sectors. Organizations in the $20B+ segment are more likely to employ CISOs with deep, sector-specific experience.

CISO job satisfaction

Large enterprise CISOs are the least satisfied with budgets followed by their compensation. Compared to other segments, CISOs in $1B – $2B firms have lower satisfaction with their level of board visibility—the share with quarterly board engagement is the smallest among these CISOs. Across all segments, most CISOs are open to changing jobs in the next 12 months.

How Security Budgets Are Allocated

As part of the survey, CISOs provided a breakdown of their security budget across eight common budget categories.

In general, staff and compensation costs account for the largest share of the large enterprise security budget (35%), followed by off-premises software, outsourcing and on-premises software.

Across segments, the budget breakdown shows several notable variations:

Enterprises in the $20B+ segment have a higher percentage for staff and compensation. This is likely a combination of companies in this segment having more employees and a tendency to pay higher salaries than firms in the other segments.

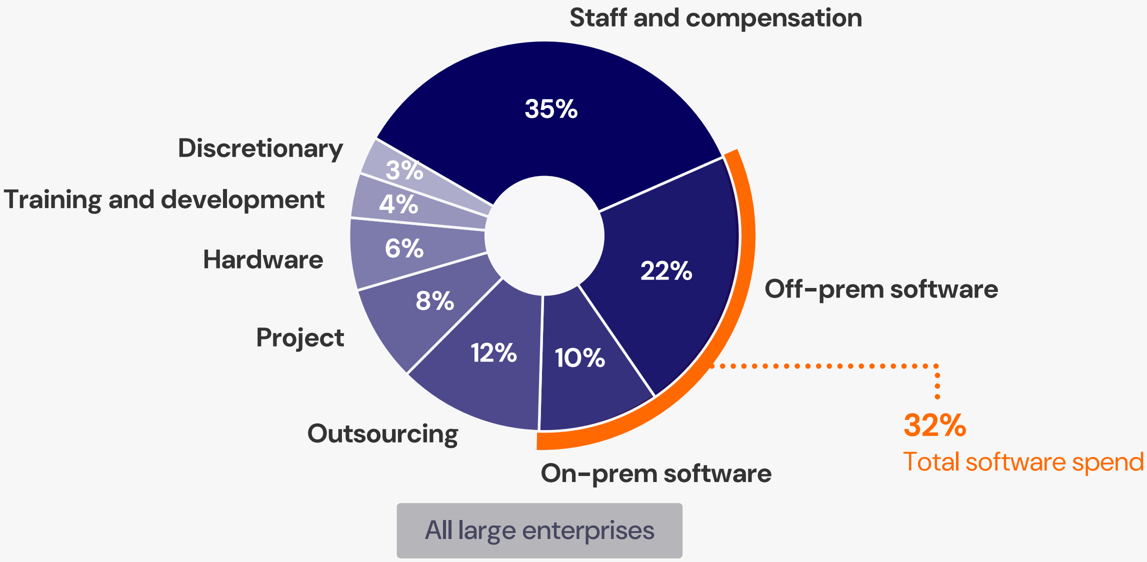
The two upper segments ($5B – $20B and $20B+) are spending a smaller share on off-prem (i.e., cloud) software and more on on-prem solutions than enterprises in the lower segments, reflecting that organizations in the upper segments often have more extensive legacy systems and tools than smaller enterprises.

This second point is tied to the degree that companies' environments, infrastructure, production and operations are based in the cloud. A budget breakdown across the large enterprise segment by degree of cloud adoption can be found in Appendix B.

Figure 1 Source: IANS & Artico Search

Large Enterprise Security Budget Breakdown

Breakdown of the annual security budget



Security budget breakdown, by segment

	$1B – $2B	$2B – $5B	$5B – $20B	$20B+
Staff/compensation	35%	35%	35%	38%
Off-prem software	25%	24%	21%	16%
On-prem software	8%	9%	11%	11%
Outsourcing	14%	12%	11%	9%
Project	7%	8%	10%	7%
Hardware	4%	5%	6%	9%
Training/development	3%	4%	4%	4%
Discretionary	3%	3%	3%	5%

Totals may not add up to 100% due to rounding.

Compensation Gaps Among Enterprise Segments

Total compensation distribution

To analyze CISO compensation within the large enterprise segment, we relied on self-reported compensation metrics: base salary, annual bonus and annual equity values.[3] Total compensation (defined as base salary plus bonus and equity) varies significantly, with the median CISO earning $532,000 and the top 10% earning over $1.4 million annually. The highest-paid CISOs are responsible for seven- to eight-figure security budgets and oversee teams of more than 200 staff. Their compensation generally includes annual equity grants averaging around $300,000, with those in the top 1% receiving multimillion-dollar equity awards annually (see Figure 3 on the next page).[4]

Annual cash compensation

Average cash compensation for large enterprise CISOs is $500,000. CISOs in the $5B – $20B segment align with this average, while those in the $1B – $2B and $2B – $5B segments typically earn below the overall enterprise average.

These compensation differences reflect the greater strategic responsibilities, broader scope and scale, and rarity of talent among the top 10% of CISOs skilled in running complex security programs and delivering enterprise-wide impact.

> “
> When discussing seven-figure annual compensation packages, CISO comp structures look more akin to executive compensation packages found in a company’s proxy statement with cash typically maxing out in the $750K – $900K range, regardless of the total annual compensation and equity making up the majority (often vast majority) of multimillion-dollar annual compensation packages.
>
> *Steve Martano*

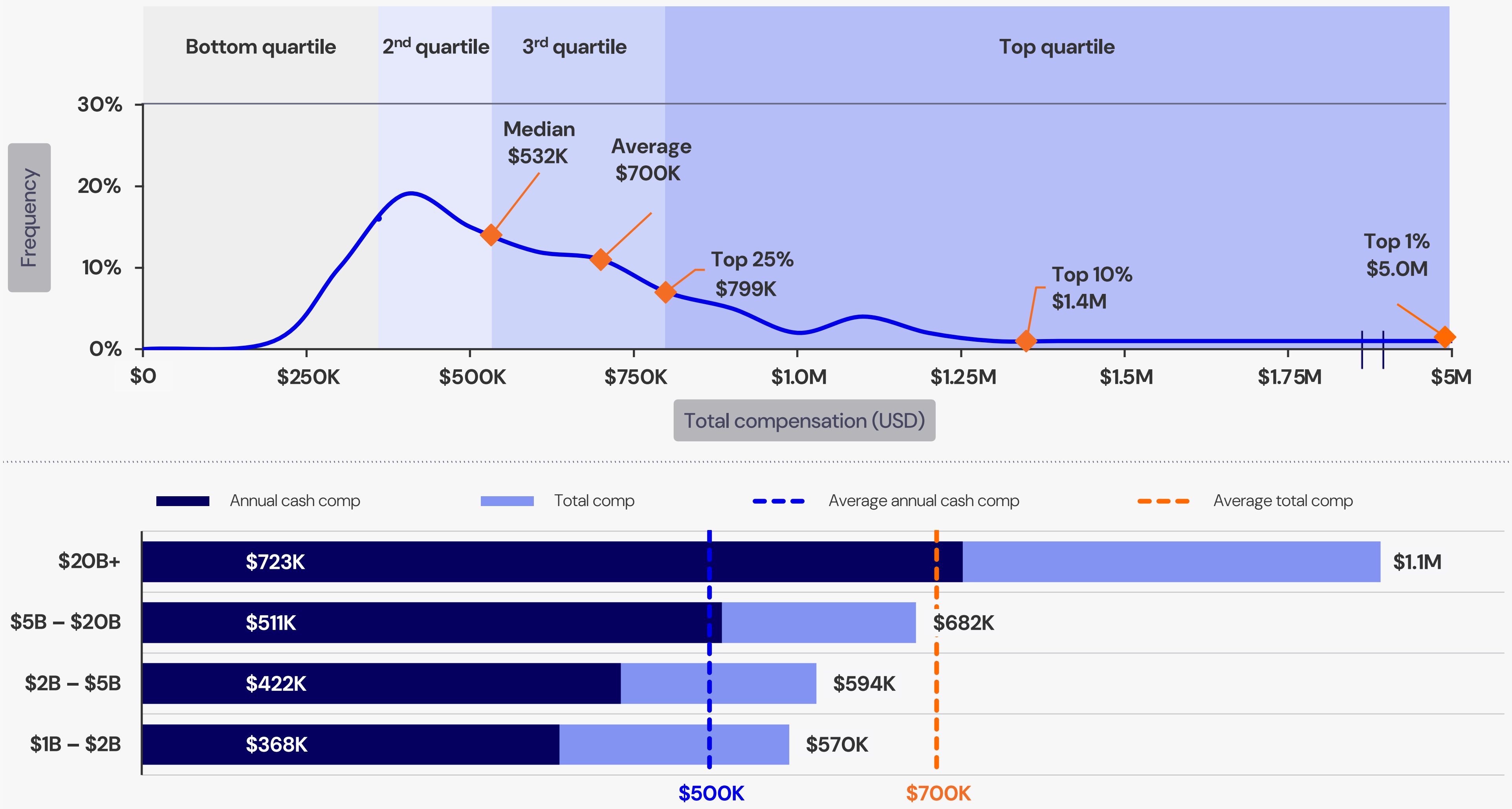
[3] To ensure a fair comparison, compensation benchmark data is limited to U.S.-based CISOs at publicly traded and privately held enterprises. We left out quasi-government and nonprofit organizations because they typically do not offer equity.

[4] For a detailed portrait of the top 10%, please see the Million-Dollar CISO infographic.

FIGURE 2 *Source: IANS & Artico Search*

U.S. Large Enterprise CISOs' Total Annual Income Spread

Total annual compensation (base salary, target bonus and equity) for U.S.-based CISOs at publicly traded and privately held enterprises



CISOs' Evolving Scope of Responsibilities

The responsibilities of CISOs continue to evolve and expand into adjacent domains.[5] These now frequently include:

Business risk
Business continuity, disaster recovery, third-party risk management and AI security.

Broader security
Product security, physical security, privacy and fraud.

IT functions
OT, IT due diligence or general IT oversight.

Digital strategy
Digital transformation and innovation.

This evolution occurs at varying speeds across organizations. There are notable differences between the large enterprise segment ($1B+) and midmarket organizations with annual revenues lower than $1 billion (see Figure 3 on the next page).

Large enterprise CISOs are less likely than their midmarket counterparts to assume full ownership of business risk, especially enterprise risk management and business continuity, as well as most broader security domains. Relatively few large enterprise CISOs have taken on IT responsibilities. In larger-scale companies, there are separate risk programs that work alongside security but are not necessarily owned by security.

These differences arise because larger companies have much greater functional specialization, allowing CISOs to focus on higher-level strategy and coordination with top executives, the board and across multiple business units, while specialized teams manage specific domains such as business continuity, risk management or fraud. In contrast, small and midmarket organizations, where executives often wear multiple hats due to leaner staffing and fewer hierarchical layers, tend to consolidate a wider range of responsibilities under the CISO.

> "Large enterprise CISO scope continues to increase as these positions evolve into more strategic risk leadership functions. Large enterprise CISOs find themselves leading broader business risk initiatives including third party risk management and AI strategy.
>
> —
>
> *Steve Martano*

[5] For more detail, please see the 2025 State of the CISO report.

FIGURE 3 *Source: IANS & Artico Search*

Large Enterprise CISOs' Scope of Responsibilities, by Segment, vs. Midmarket CISOs

What is included in your scope of responsibilities?

		Midmarket	Large enterprise			
		Less than $1B	$1B – $2B	$2B – $5B	$5B – $20B	$20B+
Infosec	Security operations	98%	96%	97%	91%	88%
	Architecture and engineering	94%	91%	95%	93%	85%
	Infosec GRC	89%	89%	92%	87%	90%
	Application security	86%	83%	89%	85%	80%
	IAM	84%	77%	81%	74%	82%
Business risk	Digital risk and compliance	95%	87%	93%	86%	87%
	Third-party risk management	88%	95%	91%	83%	78%
	Business continuity	73%	72%	51%	47%	43%
	Enterprise risk management	62%	40%	32%	31%	33%
Broader security	Product security	75%	57%	64%	61%	57%
	Privacy	54%	44%	33%	29%	27%
	Physical security	47%	26%	20%	21%	22%
	Fraud	32%	28%	25%	21%	33%
IT	Parts of IT	22%	13%	13%	10%	13%
	All of IT	22%	11%	7%	5%	3%

Less than 20% | 20% – 40% | 40% – 60% | 60% – 80% | 80%+

Large Enterprise CISOs’ Vast Experience

Years of CISO experience

On average, large enterprise CISOs have 10 years of role tenure (experience as a CISO across employers)—roughly five of which as the CISO at their current employer. The larger the company, the more years of experience: $1B – $2B CISOs average eight and a half years (across employers), while $20B+ CISOs average over 11 years of role tenure, reflecting the fact that experience is critical in being considered for CISO positions at Fortune 200-size organizations. Additionally, $20B+ CISOs stay with their current employers longer compared to their peers in other segments, with a typical difference of about two years (see Figure 4 on the next page).

Cross-sector experience

Most large enterprise CISOs have gained CISO experience across multiple companies, and many also bring cross-industry expertise. Notably, $20B+ enterprise CISOs are more likely to have multi-company experience in a single sector. These mega-cap enterprises have the resources to be more selective in their hiring and tend to prioritize candidates with deep sector-specific experience. A view into CISOs’ crossover between industry sectors can be found in Appendix C.

Career path

The predominant pathway to the CISO role has historically been through IT, with more than 75% of respondents having backgrounds in IT infrastructure, architecture and engineering, development and operations, and/or security and operations. Compliance backgrounds (such as governance, risk management and compliance; audit/risk assessment) are more common among $1B – $2B CISOs (22%) than among $20B-plus CISOs (12%), likely reflecting the broader range of skills and experiences sought by smaller organizations. CISOs with long tenures—a group with higher representation in the $20B+ segment—typically have backgrounds in tech, because in security’s early days, when many of these CISOs embarked on their careers, compliance wasn’t a formal function yet. In contrast, the $1B – $2B segment has relatively more CISOs with shorter tenures who started their careers later in time and were able to follow a formal compliance career path.

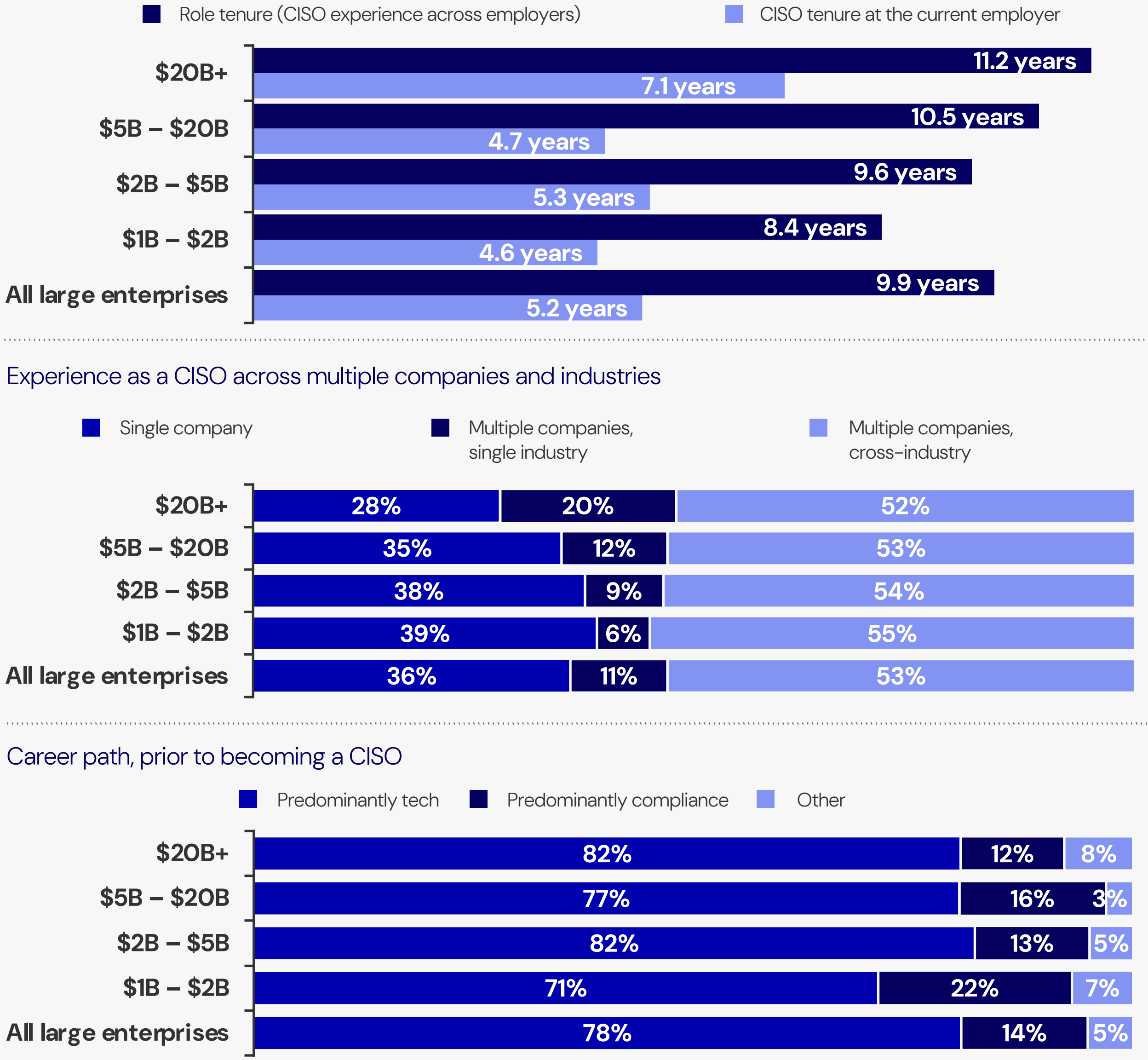
> “
>
> One of the challenges CISOs face is they have only reported to tech, led technical teams and managed technical budgets. When elevating to an enterprise CISO role, the position is less about technical acumen and more about business risk and business alignment. In some respects, the market is training technical leaders in a way that is mismatched from the aspired job of CISO.
>
> —
>
> *Matt Comyns*

FIGURE 4

Source: IANS & Artico Search

Large Enterprise CISOs' Background and Experience

What is your background before becoming a CISO and your experience as a CISO?



Experience as a CISO across multiple companies and industries

Career path, prior to becoming a CISO

"Other" includes law enforcement, military and national security

Job Satisfaction of Large Enterprise CISOs

Low marks for budget

The survey asked CISOs to rate their job satisfaction across four key areas: security budget, compensation, their visibility with the board and career development. Satisfaction with budget received the lowest ratings overall, particularly among CISOs in the $1B – $2B and $5B – $20B segments— a reflection of frustration at being expected to do too much with not enough resources.

Mixed satisfaction for compensation and board visibility

Both $20B+ and $1B – $2B CISOs reported below average satisfaction with their compensation, though for different reasons.

CISOs in the $20B+ segment likely compare their pay to that of other executive leaders within their organizations and consider their compensation insufficient given the demands and increasing scope of their roles. CISOs in the $1B – $2B group, meanwhile, may feel their compensation is falling behind that of their peers in the wider large enterprise segment. This group is also the most dissatisfied with their level of visibility and engagement with the board, corresponding to the outsized share (24%) of CISOs in this segment with little-to-no board engagement.

FIGURE 5 Source: IANS & Artico Search

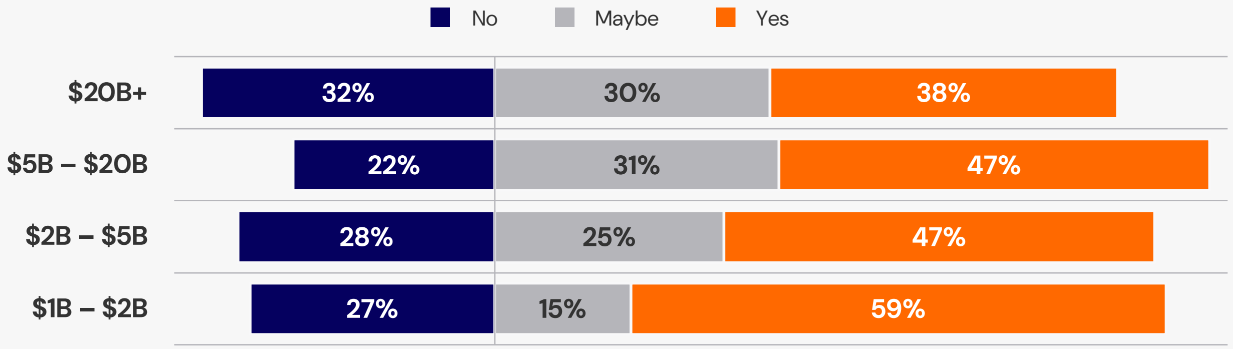
Large Enterprise CISOs' Satisfaction With Their Job

Share of CISOs satisfied with key job aspects and the share considering a job change in the next 12 months

	Budget	Compensation	Board visibility	Career development
$20B+	58%	55%	67%	63%
$5B – $20B	52%	63%	66%	63%
$1B – $5B	55%	60%	63%	71%
$1B – $2B	51%	57%	59%	66%

Less than 55% | 55% – 59% | 60% – 64% | 65% – 69% | 70%+

CISOs considering a job change in the next 12 months



Considering new opportunities

$20B+ CISOs have the longest-average tenure at their current company (averaging 7.1 years); a third of them indicated they are not considering a job change in the next 12 months—a higher proportion than in other enterprise segments. Conversely, the $5B – $20B segment has the largest share of CISOs who are open to new opportunities, as indicated by those who answered "maybe" or "yes" when asked about a potential employer change.

Recommendations for Coping With Common Challenges

This section focuses on three key challenges that most CISOs at large enterprises face at some point in their career. Our team of experts offers recommendations for managing each.

1 Scope creep and functional expansion

Most large enterprise CISOs have already experienced a growing scope of responsibilities in recent years, now commonly owning business risk functions like digital risk and compliance and/or third-party risk management. This trend is likely to persist with regard to accountabilities already commonly held by midmarket CISOs, such as privacy, physical security and fraud—and possibly also new, adjacent domains including digital strategy and IT functions or the secure use of AI-powered automation. As their organizations grow, and especially when a vacuum arises due to the departure of another executive leader, CISOs may be called upon to take on additional responsibilities.

Recommendations

- ✓ As these opportunities arise, as the CISO you should carefully evaluate the strategic implications and your ability to add value. Taking on additional scope can better position you as a critical enterprise leader, but it can also be a distraction from your core cybersecurity responsibilities. Be mindful of maintaining clear boundaries and ensuring you have the necessary resources and support to effectively manage these expanded responsibilities.

- ✓ You can leverage meaningful increases in job scope for compensation and title advancement. We recommend using third-party data to understand and benchmark your scope, title and compensation against peers and market standards. Quantify the additional responsibilities you're asked to assume and show how the additional scope adds strategic value to the organization. The key is to be proactive, data-driven and strategic in how you present your evolving role's value to the organization.

> “CISOs can leverage scope creep to garner more cross-functional visiblity and serve as a thought-leader in emerging areas. Practitioners would be wise to get in front of AI strategy discussions because it's easier to get security's perspective upfront rather than after a decision has already been made.
>
> —
>
> *Steve Martano*

2 Transitioning to a “strategic relationship executive”

At larger organizations, especially in more cyber-mature industry sectors like financial services and tech, many CISOs have transformed from a hands-on technical manager to an executive, where the focus shifts from directly handling security implementation to building and managing complex cross-functional relationships with peer executives in IT, privacy, risk management and legal, as well as with functional department leaders, country managers, the executive leadership team and the board of directors. While this may sound “easy,” it involves a lot of “soft skills”—wielding influence not authority, executive communications, coaching and partnership—that CISOs have not needed to build or demonstrate while climbing the ladder of the cybersecurity organization. Key characteristics of this relationship-driven approach include acting as a trusted advisor to senior leadership, developing deep connections with other senior leaders, and navigating organizational politics and competing priorities.

Recommendations

- ✓ Given this is a gradual shift and new expectations are often implicit rather than hard goals, we recommend CISOs plan for their own soft skill development, especially in areas of communication, influence and self-advocacy.
- ✓ Invest heavily in communication skills that translate complex security concepts into business language, positioning yourself as a trusted advisor rather than a tactical manager.
- ✓ Cultivate a mindset of business leadership, where security is viewed as an enabler of organizational objectives rather than a stand-alone technical function.
- ✓ Start to develop a more senior and strategic network.

3 Career pathing and mobility planning

Navigating CISO career paths requires sophistication, particularly when considering cross-sector moves or scaling to larger organizations. Moving among sectors is nuanced: highly regulated industries like financial services and healthcare often prefer candidates with sector-specific experience, while less-mature sectors seek CISOs from industries with more-advanced cybersecurity standards to drive program maturity. Transitioning to larger companies is challenging, with most organizations preferring CISOs who have already held the title at comparable (or larger) organizations, or those from prestigious "blue chip" tech companies. Successful career progression demands a careful assessment of role seniority, compensation trajectory and alignment with long-term career objectives, requiring CISOs to be discerning about the realizable potential of each opportunity, rather than accepting job promises at face value.

Recommendations

- ✓ To effectively manage career pathing and mobility, you should evaluate potential roles not just by title or immediate compensation, but by their alignment with your long-term career objectives and potential for transformational impact. Be prepared to make calculated moves, potentially taking intermediate steps like moving to a larger organization's secondary security role or transitioning through different sectors over a longer time period to build comprehensive experience.

- ✓ When considering a role in an industry that's considered less cyber-mature, prospective employers may make grandiose claims to attract top talent. You should seek to validate such claims to understand potential employers' commitment to cybersecurity, such as by asking about budget growth commitments, leadership's understanding of gaps in the current security program, and determining if they want incremental improvements or a fundamental overhaul of the security program.

Methodology

IANS and Artico Search fielded their fifth annual CISO Compensation and Budget survey in April 2024. From April until December, we received survey responses from 862 security executives at a diverse set of companies with regard to size, location and industry. Of them, 406 were categorized as large enterprises, with the following breakdown:

- **$20B+ annual revenue:** 15%
- **$5B – $20B:** 31%
- **$2B – $5B:** 34%
- **$1B – $2B:** 20%

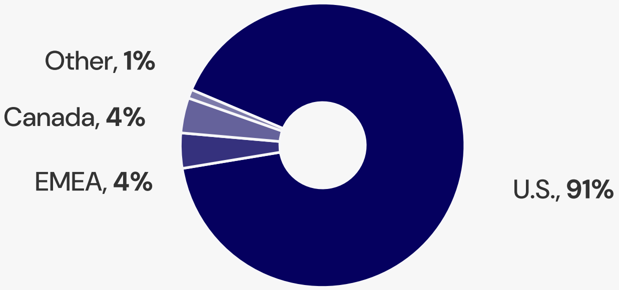
FIGURE 6 *Source: IANS & Artico Search*

Large Enterprises Sample Breakdown: N = 406

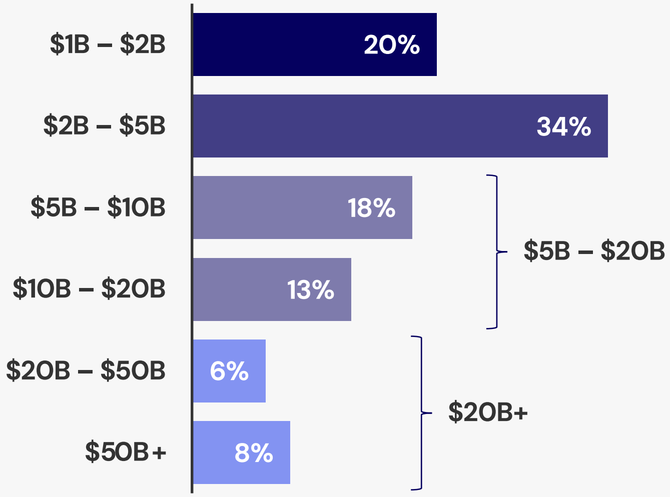
Ownership type

	Quasi-government/ nonprofit	Privately owned	Publicly listed
$1B – $2B	12%	42%	46%
$2B – $5B	17%	30%	54%
$5B – $20B	9%	23%	68%
$20B+	11%	18%	71%

CISO primary work location



Annual revenue



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.