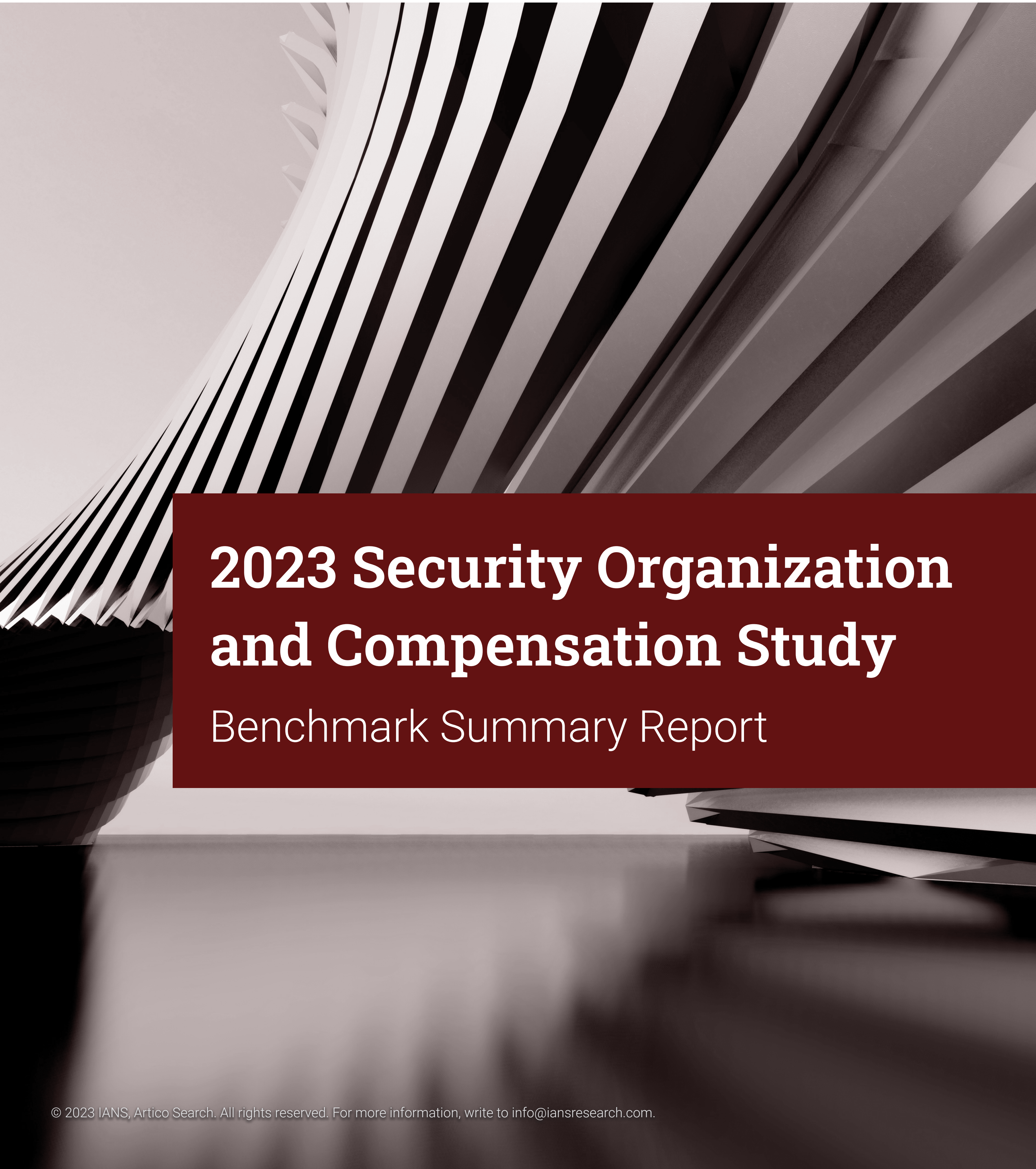
IANS + ARTICO



2023 Security Organization and Compensation Study

Benchmark Summary Report

Table of Contents

This summary report provides high-level insights from our 2023 Security Organization and Compensation Benchmark Study.

The complete 2023 Security Organization and Compensation Benchmark 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

Executive Summary

The success of an organization's security strategy depends on both the proper sizing of the security team and the caliber of the talent within it. CISOs take particular care in timely adding functional department leadership positions to their org and hiring the best leader talent their budget allows, because they directly shape the security team performance.

In anticipation of the needs of the wider organization, CISOs must make org and staffing decisions which are dynamic and influenced by market conditions, growth objectives, acquisition strategies and regulatory changes, to name a few.

By aligning their security org with the needs of the broader organization—both current and future state—CISOs avoid overburdening their teams, a well understood cause of dissatisfaction and attrition driver.

Research into cybersecurity org planning

We analyzed security org planning decisions, such as the installation of functional leaders at various organizational milestones and the compensation rates and corporate levels for key positions. For this, we used data from 1,195 CISOs, cybersecurity leaders and staff. The CISOs responded to the 2023 CISO Compensation and Budget survey. Functional leaders and staff members took the 2023 Cybersecurity Staff and Career survey.

This report presents the key findings of the research. We included perspectives from executives at Artico Search, in particular Matt Comyns, co-founder and president, and Steve Martano, partner in Artico Search's cyber practice. This combination of data and expert insights provides a thorough view into organizational design decisions and leadership compensation.

3 commonly implemented org designs

We found three overarching organizational designs:

Fortune firm security org designs with four or more layers of management and 50-plus full-time equivalents (FTEs). About 25% of these designs have a global CISO and roughly a third have a named deputy CISO supporting the CISO manage the broad scope and complexity of the security agenda and who serve as heir apparent to the CISO.

Large enterprise security org designs with 10 to 50 staff spread over two or three management layers, which typically include dedicated leaders for SecOps; governance, risk management and compliance (GRC); architecture and engineering (A&E); and/or IAM who manage their own teams of individual contributors. Most of these orgs use MSSPs.

Midsize company security org designs with a small, focused team of up to 15 FTEs who handle essential security measures collectively. Each team member generally supports multiple functions within the security stack.

Successful hiring and retention of cyber leaders hinges on the right comp plans

CISO respondent data regarding critical cybersecurity hires suggests acquiring and keeping talent is the toughest for leaders in the SecOps and application security (AppSec) domains—SecOps, because it is typically the first function for which CISOs appoint a functional leader, so demand runs high, and AppSec, because of the growing number of CISOs appointing their first leader for this function in response to strengthening customer demand for app security.

CISOs and the talent managers who support them need to be cognizant of more than just market rates for the various leadership roles. More importantly, they should familiarize themselves with the top-25% comp brackets, regardless of the type of org design—from Fortune firm org designs that need mature leaders who are experienced with scope and complexity to large enterprise and midsize company org structures that need leaders with broad experience to be able to lead across multiple functions. Understanding the top of the market provides vital context to help CISOs set the right compensation band for the role they are trying to fill.

> *"We recommend CISOs benchmark their team's comp against market rates such that, when filling a vacancy, they know what type of candidates fit the available comp band and the corresponding talent levels they yield."*
>
> ***— Matt Comyns, Artico Search***

Security Org Designs for 3 Revenue Segments

In general, there is a positive correlation between revenue size of the overall organization and size and complexity of the cybersecurity organization.

Hence, for our analysis, we grouped respondents by the size of their company. We then identified common elements of their security teams and org structure. That resulted in three distinct org designs, each with a corresponding annual revenue range, as laid out in Figure 1.[1]

FIGURE 1

3 Security Org Designs Corresponding With 3 Revenue Segments

Three types of security orgs befitting to three types of companies, based on their annual revenue

Security org type	Annual revenue range	Security Characteristics	Security budget range	Security FTE range
Fortune firm	More than $6B	• Highly complex security requirements • Large and specialized security workforce covering comprehensive security measures	More than $10M	More than 50
Large enterprise	$400M – $6B	• Moderate to substantial security requirements • Dedicated security team responsible for a range of security functions	$2.5M – $10M	10 to 50
Midsize company	$50M – $400M	• Limited security requirements • Small, focused security team handling essential security measures	$1M – $5M	Fewer than 15

[1] FIGURE 1 illustrate each of these org designs. We should note that while they are based on the commonalities we found in the data, situational nuances are possible

Fortune Firm Security Org Design

Figure 2 illustrates the key characteristics of the Fortune security org designs, often with operations that span multiple divisions and countries.

FIGURE 2

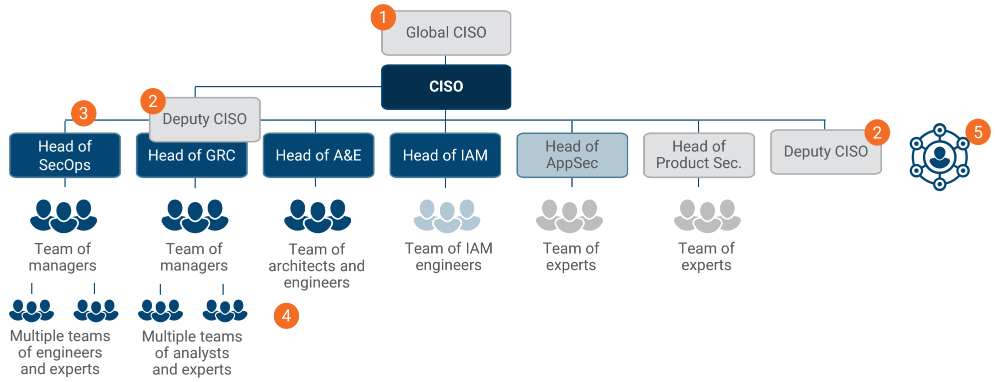
Fortune Firm Security Org Design

A typical security org design for companies with more than $6B (USD) in annual revenues

	Annual revenue	Security FTEs	Security budget	Layers beneath the CISO
Range	$6B+	50+	$10M+	4 or more

% who have this role or team

- <25%
- 25% – 49%
- 50% – 74%
- 75%+



1. **At 24% of Fortune firms, the top cyber role is a global CISO.**

   Most Fortune firm CISOs and global CISOs are VP-level or higher (see Figure 2.1).
   74% of CISOs and global CISOs report to a CIO or CTO.
   The other 26% report to a business function such as a COO, CFO, chief risk officer or legal counsel.

2. **The deputy CISO is typically the CISO's successor.**

   It can be a stand-alone role that helps the CISO by sharing in the workload.
   It can be also an overlay role that combines with, for example, the head of GRC role, with a title such as director of GRC and deputy CISO.
   They are seasoned leaders with 12+ years of cyber experience.
   44% are director level; 50% are VP or higher.

3. **SecOps, GRC and A&E have dedicated functional leaders at 75%+ of Fortune companies.**

   The product security function with a dedicated leader is common in the tech sector.
   The AppSec function and leader are common in the finance, tech and retail sectors.
   8 out of 10 Fortune-firm functional leaders are director level or VP level (see Figure 2.2).

4. **Most functional teams range from 15 to 30 FTEs.**

   The SecOps and GRC teams are most likely to have an additional managerial layer.

5. **75% use MSSPs.**

   4 in 10 CISOs spend between 5% to 10% of their budget on outsourcing; 1 in 5 spend between 11% and 20%.

Figure 2.1
Organizational Level of Fortune Firm CISOs

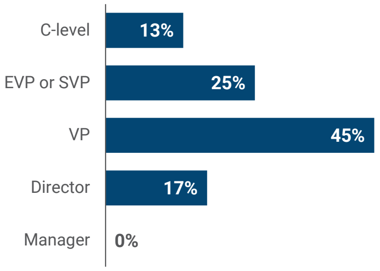
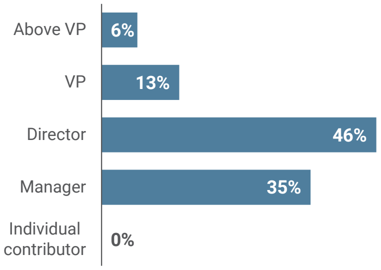


Figure 2.2
Org Level of Fortune Firm Security Leaders



Cybersecurity leader compensation variations by industry

Comparing leader role comp packages with annual equity and those without across five key sectors, the data shows that finance cyber leaders have the highest average comp. This sector averages a higher base salary and bigger bonus and equity percentages than the other industries.

On average, the leaders with equity (generally, at the direct level or higher) earn $135,000 more annually than those without. This difference is greatest among finance, healthcare and manufacturing respondents. In retail, the comp, especially cash comp, of both groups are more aligned.

More than half of leaders at the VP level or higher receive annual equity

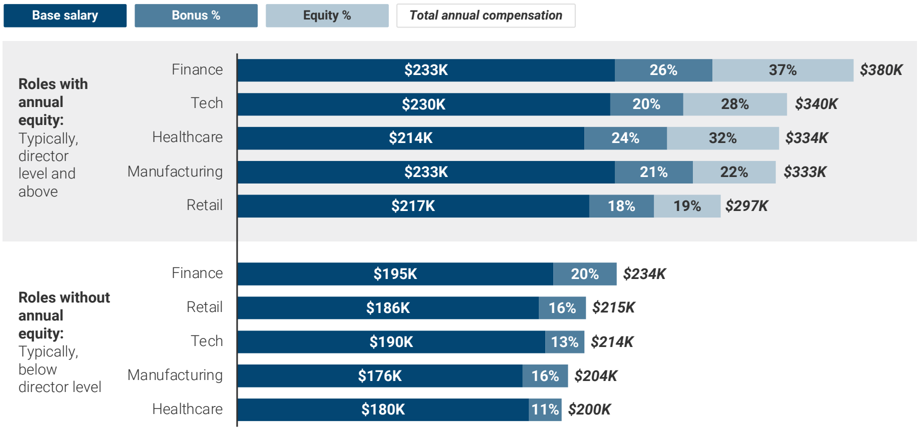
Regardless of org design, eligibility for annual equity correlates positively with the organizational level of a role. About a quarter of functional leaders who are below director level (managers, supervisors or individual contributors) receive annual equity.

In contrast, 60% of director-level leaders qualify for equity packages and, roughly, 65% of those are VP level or higher (SVP or EVP).

FIGURE 3

Cyber Leader Compensation Variations Across Sectors

Base salary, target bonus, equity and the calculated annual total compensation in USD



Org Design Differences by Industry

In this section, we look at differences in org design at various stages of growth—measured in annual revenue. It focuses on the management layer of the cybersecurity organization that reports to the CISO. The org charts are based on responses from 660 CISOs about leadership positions in their management teams.

An industry-agnostic cybersecurity management org chart shows that at $100 million in annual revenue, between a quarter and half of CISOs indicate they have leadership positions in their org for one or more of the functions SecOps, GRC, A&E and product security.

At the next revenue milestone, $500 million, the presence of leadership positions for SecOps, GRC and A&E grows to between 50% and 74% of CISOs.

The head of SecOps role is the first role that's a standard fixture, generally at the $1 billion revenue milestone. At the $10 billion threshold, the same is true for GRC and A&E.

At $25 billion, most companies also have a head of AppSec and a deputy CISO (see Figure 4).

FIGURE 4

Security Org Design at Different Revenue Milestones

Typical security leadership team structure in FTE for various revenue levels in USD

Revenue milestone and average security FTE range

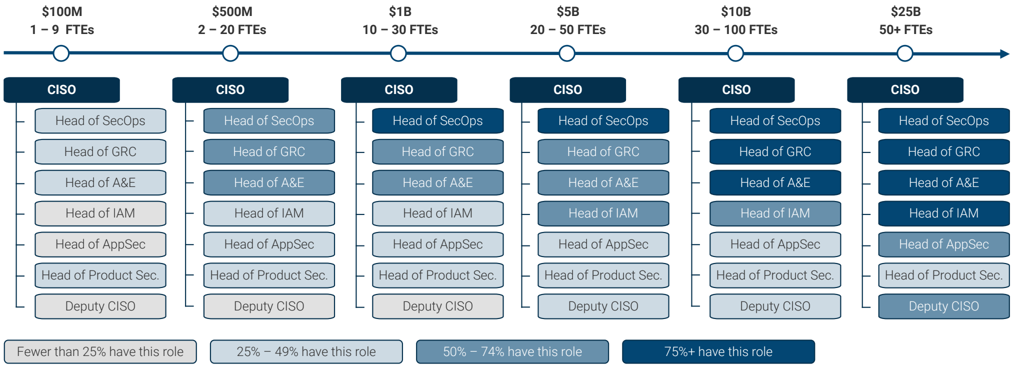
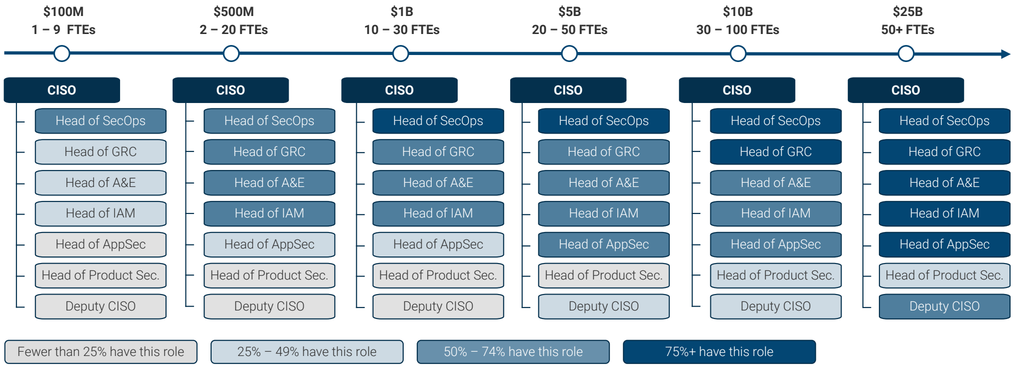


FIGURE 5

Finance Security Org Design at Different Revenue Milestones

Typical security leadership team structure in FTE for various revenue levels in USD

Revenue milestone and average security FTE range



Finance cyber leadership orgs appoint a SecOps leader earlier than average

At $100 million, more finance firms have a head of SecOps than average. The head of IAM appears at earlier revenue milestones in this sector compared with the overall sample, while fewer finance firms have an immediate need for a head of product security (see FIGURE 5).

Steve Martano explains:

> *The banking sector was a 'first-mover' in designing internal cutting-edge SOCs—a trend that has continued in the sector. Compared to other sectors, financial services firms typically design and build an in-house SecOps function, rather than outsource it to an MSSP.*

Tech cyber leadership orgs are more comprehensive at earlier milestones than average

Even at $100 million in revenues, between 50% and 74% of tech CISOs have heads of SecOps, GRC and/or A&E. Another key difference between tech cyber leader orgs and the generic orgs is the installation of a head of product security and head of AppSec at relatively early revenue milestones in the majority of cases (see FIGURE 6).

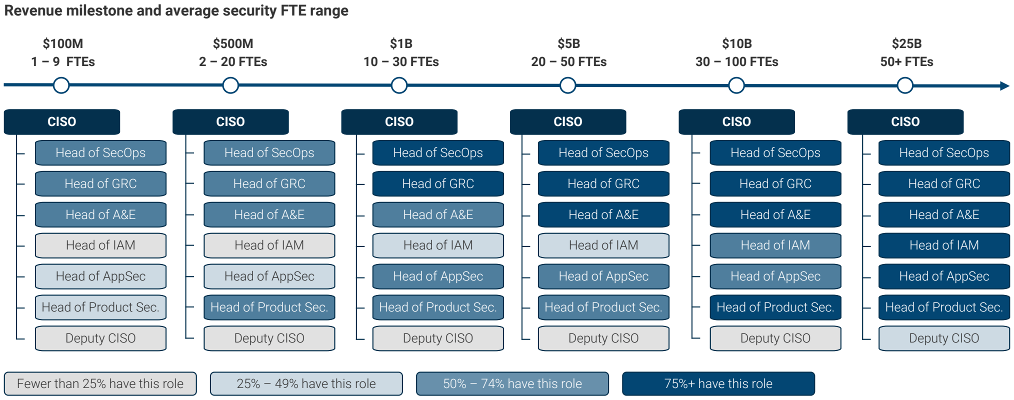
Steve Martano explains why security is such a focus for tech orgs:

> *Due to external pressures, product-centric tech organizations are increasingly integrating security into DevOps at an earlier stage in the company's lifecycle. Customer requirements, increased investor scrutiny and aspirations for a transaction such as an initial public offering all keep security top of mind for senior leaders as a company scales.*

FIGURE 6

Tech Security Org Design at Different Revenue Milestones

Typical security leadership team structure in FTE for various revenue levels in USD



In manufacturing, cyber leaders are added at higher-revenue thresholds than average

Unlike the cross-industry org design, in manufacturing, none of the leadership roles see 75% or higher penetration rates at the $1 billion or $5 billion revenue thresholds.

That changes only at the $25 billion revenue milestone. By then, four roles—the heads of SecOps, GRC, A&E and IAM—are on the org charts in at least 75% of manufacturing firms.

Steve Martano elaborates on sector-specific organizations' priorities:

> *In budget allocation, industry-specific needs play a crucial role. For manufacturers with asset-rich plants, we find CISOs need to prioritize security in areas such as IoT, IT/OT and industrial control systems.*

Most retail cyber management teams start with a head of SecOps

At the $1 billion revenue milestone, nearly all retail CISOs have hired a head of SecOps and most have a head of GRC role on their org chart. The leaders added on most retail org charts are the heads of A&E and IAM. Across the milestones, 25% to 49% of retail org charts have a head of AppSec.

Most CISOs' Have Hiring Needs For Leadership Roles

The data indicates that, across sectors, roughly 15% are at or approaching a revenue milestone that warrants the addition of a head of SecOps to their security organizations, based on what is typical for their peer group.

Another 4% of CISOs indicated they have the SecOps leader role in their org charts that is currently vacant with a critical need to fill. That makes for a total of 19% of CISOs looking for a head of SecOps in the immediate or near future.

For 15% of CISOs, a head of AppSec is a likely or critical hire, followed by 13% for a head of IAM. For the deputy CISO and product security leader, the share of CISOs with hiring needs is lower at 5% and 3%, respectively (see FIGURE 7).

The top 25% averages $523K in total comp

CISOs' hiring and retention strategies generally revolve around recruiting and keeping the best talent. For this, they focus on the top quartile comp, rather than the median or average market rates.

This section provides median, top-25% and top-10% compensation for cybersecurity leader roles in the U.S. We filtered out the comp packages that do not include annual equity.

To understand the top quarterly pay range, we calculated the top-25% floor—the entry point for the top quartile, the top-25% average and the top-10% average (see FIGURE 8).

FIGURE 7

Share of CISOs With Hiring Needs

Share of CISOs considering adding new leadership roles and those with critical need to hire for existing leadership roles

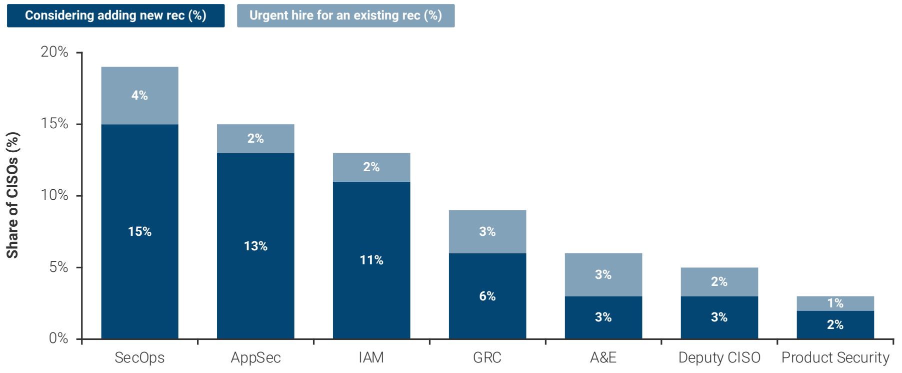
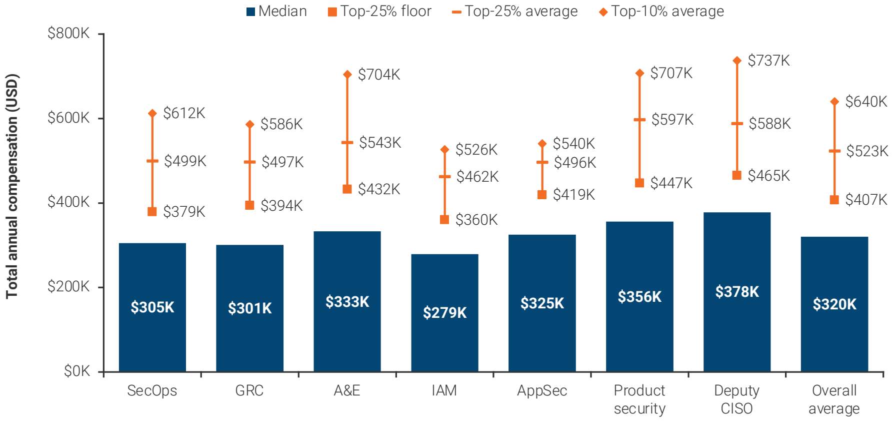


FIGURE 8

The Top-25% Total Compensation by Functional Leader Role

Calculated total annual compensation, including base salary, target bonus and equity (USD, thousands)



The top-25% range for total comp starts at $407,000 and has an average of $523,000. The top-10% average is $640,000. For the deputy CISO, the head of product security and the head of A&E, the top-10% figures exceed $700,000.

The heads of SecOps, GRC and AppSec in the sample have top-25% averages for total compensation just shy of $500,000.

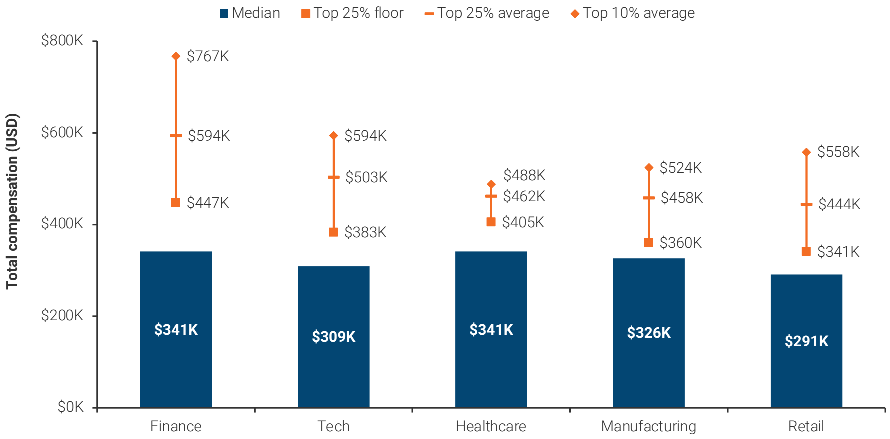
Security leader compensation variations across industry sectors

Across sectors, finance and healthcare firms have the highest median annual total compensation at $341,000. But the top-25% and top-10% averages in finance exceeds that of the other sectors at $594,000 and $767,000, respectively (see FIGURE 9).

FIGURE 9

The Top-25% Leadership Roles' Total Compensation by Industry

Calculated total annual compensation, including base salary, target bonus and equity (USD, thousands)



Conclusions

Highlights from the research are:

CISOs make distinct org decisions at different stages of company growth

At different levels of size and scale, the security needs and corresponding organizational designs differ. Fortune firms with annual revenues exceeding $6 billion operate large and specialized security orgs with four or more management layers, often with a global CISO who heads up the companywide security org. The dedicated functional department generally has 12-plus years of domain experience and receives comp packages that include annual equity.

Smaller organizations with more limited security requirements scale their security organizations accordingly. A typical feature at midsize companies with annual revenues between $50 million and $400 million is leadership roles with multifunctional responsibilities, as well as staff—analysts, architects and engineers—who wear multiple hats.

To attract and retain key talent, advocate for budget in the top-25% comp ranges

Fortune firm security orgs need leaders who are experienced with complexity and scale. The market rates for these leader roles are higher than for those in large enterprises and midsize companies. What's more, the top 25% has an overall comp that averages about $200,000 more than the median comp.

While hiring in the top 25% doesn't guarantee top performance, when an organization considers its talent to be in the top quartile for pay, they generally also perceive them as top-quartile performers in their respective roles.

Methodology

IANS and Artico Search fielded the fourth annual CISO Compensation and Budget survey in April 2023. This year, we expanded the survey to include a dedicated set of questions for staff—including analysts, architects, engineers, managers, experts and functional leaders. From April until August, we received survey responses from 663 CISOs and 532 staff members from companies that varied by size, location and industry.

We combined the data from both groups to determine the decisions made for the security organizations at small and midsize companies (with annual revenues of between $50 million and $400 million), large enterprises (with an annual revenue ranging between $400 million and $6 billion), and very large and global enterprises (with annual revenues exceeding $6 billion). The $6 billion cutoff for very large and global enterprises is the annual revenue of the 500th company in the Fortune 500 in May of 2023, midway through the survey.

Unbiased research

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.

The main activities involved in the research include:

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

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.

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

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.

Sample breakdown

Of the sample of 663 CISOs, 566 work in the U.S. and 43 work in Canada.

The distribution of CISOs among the three sizes of companies represented in this report is roughly equal, with each representing about a third of the sample of CISOs.

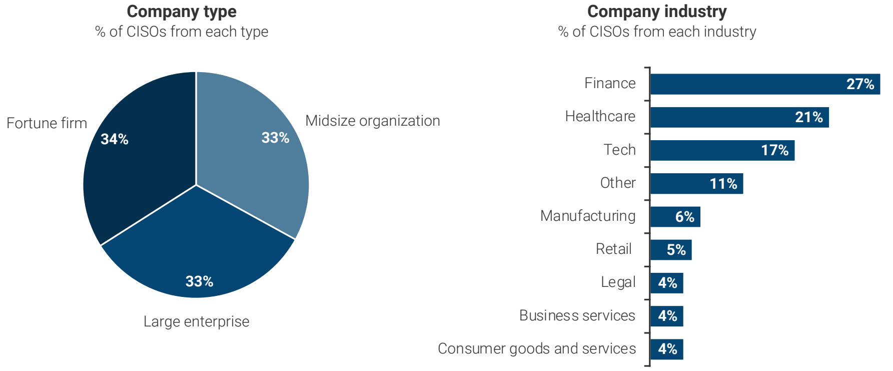
The three largest industries in terms of representation among CISOs in the sample are finance (27%), healthcare (21%) and tech (17%). FIGURE 10 shows the sample breakdown along size and sector dimensions.

Of the sample of 532 staff members, 34% are functional department heads (i.e., functional leaders), 22% are analysts, 19% are engineers, 16% are architects and 5% are managers (see FIGURE 11).

FIGURE 10

CISO Sample Breakdown

Breakdown of 663 respondents to the 2023 CISO Compensation and Budget Survey

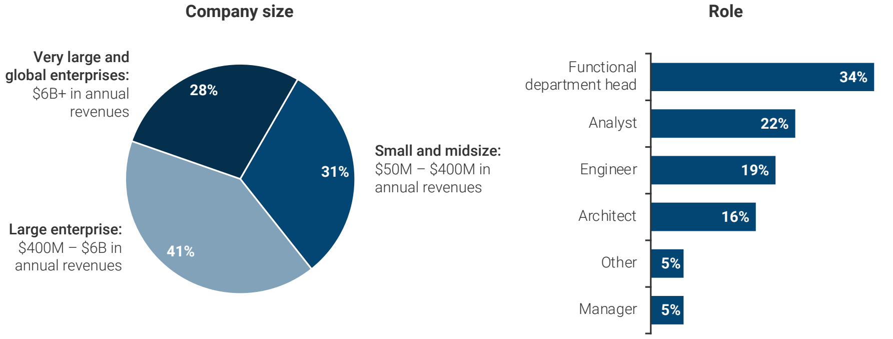


The "Other" category includes transportation, utilities, education and government. Percentages may not add up to 100% due to rounding.

FIGURE 11

Cybersecurity Staff Sample Breakdown

Breakdown of 532 respondents to the 2023 Cybersecurity Staff and Career survey



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

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.