HITCH PARTNERS

GLOBAL SECURITY LEADERSHIP ANALYSIS

2026 Global CISO Leadership Report

Executive analysis of compensation, reporting structures, AI governance, and strategic priorities across 625+ security leaders.

$128K
PUBLIC COMPANY - PRIVATE COMPANY GAP

2%
OPTIMIZED AI GOVERNANCE

43%
CISOS REPORT THIRD PARTY RISK AS TOP PRIORITY

EXPLORE

Introduction & Methodology

Introduction

Presented by **Hitch Partners**, the 2026 Global Organization Report analyzes the evolving landscape of security leadership. Now in its ninth annual edition, the report provides critical insight into compensation trends, reporting structures, and the expanding responsibilities of security executives in 2025.

This year's analysis examines both Chief Information Security Officers (CISOs) and NextGen security leaders. While CISOs continue to shape security strategy and communicate risk at the executive level, NextGen security leaders who operate just below the CISO are playing an increasingly pivotal role in executing strategy, owning key security programs, and driving operational excellence.

As threats to infrastructure and applications intensify, demand for seasoned security leadership remains high. Both CISOs and NextGen security leaders are commanding competitive compensation as organizations prioritize security at the highest levels.

Hitch Partners specializes in executive search and sector advocacy, equipping security leaders with data-driven insights to navigate this dynamic field. We welcome your feedback and invite you to share topics you'd like us to explore in future reports.

625+
SURVEY RESPONDENTS

9th
ANNUAL EDITION

93%
NORTH AMERICAN COVERAGE

Methodology

This report is based on survey responses from more than 625+ Information Security executives across North America (U.S. and Canada) and select international markets. Responses were collected between Q4 2025 and Q1 2026 and represent a broad cross-section of industries, company sizes, and organizational models providing a comprehensive view of how security leadership is evolving as we enter 2026.

Scope & Definitions

"CISO" Definition: Throughout this report, CISO refers to the most senior security leader accountable for an organization's information security strategy, program execution, and risk management. This encompasses multiple titles, including:

- Chief Information Security Officer (CISO)
- Chief Security Officer (CSO)
- Head of Security / Head of Information Security
- Vice President of Security / VP of Information Security
- Senior Director of Security (when serving as top security role)

"NextGen" Definition: "NextGen" refers to the security leadership layer directly reporting to the CISO—typically the top 3-5 security leaders responsible for executing the security program across specialized domains. These roles represent the next generation of CISO talent and include titles such as:

- Deputy CISO
- Head of Security / Security Engineering
- Vice President of Product Security / Application Security
- Senior Director / Director of Security (domain-specific: Cloud, Identity, GRC, etc.)

NextGen leaders translate CISO strategy into operational execution, combining strategic alignment with hands-on program leadership. They typically manage teams of 5 to 50+ security professionals within their areas of specialization.

Geographic Segments

This report highlights the North American security leadership market, a space Hitch Partners has supported through security leadership searches for more than a decade. With respondents based in the U.S. and Canada, the dataset offers a robust regional view of compensation benchmarks, organizational structures, and evolving security priorities.

Expanding Global Coverage: Beginning in 2025, we expanded our data collection beyond North America to include European and broader international markets to establish baseline benchmarks and better understand regional differences in security leadership practices. While

international respondents currently account for a significantly lower percentage of total responses, we are committed to increasing global representation in future editions.

Current International Representation:

- European Union: Concentrated in Germany, France, and the Netherlands
- United Kingdom: London, other major business centers
- Scandinavia: Norway, Sweden, Denmark
- Middle East: UAE, Saudi Arabia, and Israel
- Australia: Sydney and Melbourne metro areas

As the international dataset matures over the next 12–24 months, we will introduce deeper regional analysis, including market-specific compensation benchmarks, regulatory drivers (such as GDPR, NIS2, and DORA), and structural differences in security organizations. In this year's edition, international findings are presented alongside North American data where sample sizes support statistically meaningful comparisons. All international compensation figures have been converted to USD using exchange rates as of January 11, 2026, to ensure direct comparability.

Acknowledgment & Thanks

We extend our sincere thanks to the security leaders who contributed their time and insight to this report, and to the broader community who helped rally participation across North America and international markets. This benchmark exists because of your engagement and trust.

We are grateful to the many CISOs and security leaders we connected with throughout the year at CISO Sanctuary gatherings, speaking engagements, our annual Brewery Party, Black Hat, and other industry events around the world. These conversations continue to shape our perspective and strengthen this community.

We also want to recognize and thank the Hitch team for the care, rigor, and coordination behind this effort - from research and analysis to community outreach and execution.

We look forward to even deeper engagement in 2026 and remain committed to supporting and advocating for a security leadership community we truly admire and care about.

EXECUTIVE SUMMARY

Critical Inflection Points in Security Leadership

The 2026 Global CISO Report reveals fundamental shifts in compensation, reporting structures, and governance with implications for every security leader's strategic positioning.

$128K
PUBLIC COMPANY VS PRIVATE COMPANY COMPENSATION GAP

30-32%
CISO REPORT TO CTO / ENGINEERING

2%
HAVE OPTIMIZED AI GOVERNANCE

36%
PRIVATE COMPANY CISOS WITHOUT LIABILITY PROTECTION

43%
CISOS REPORT THIRD PARTY RISK AS #1 PRIORITY

+6% YoY
NEXTGEN COMPENSATION GROWTH OUTPACING CISO

Based on responses from 625+ information security executives collected Q4 2025–Q1 2026, this analysis identifies the critical decisions facing security leadership in 2026.

SECTION 01

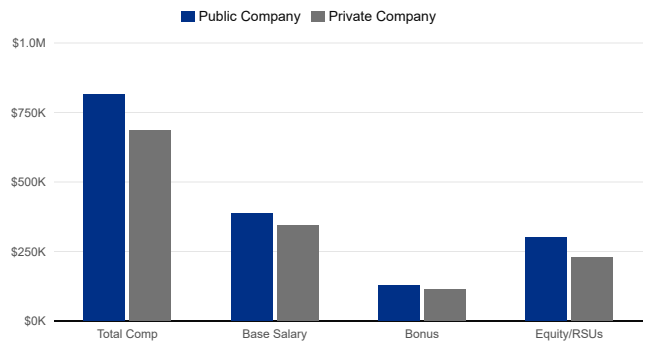
Compensation Analysis

Public companies maintain significant compensation advantages across all components, with equity driving the largest differentials.

Public vs. Private Company CISO Compensation

Total compensation breakdown reveals structural differences in how organizations value security leadership.

Public vs Private | Gender Pay Gap



$814K

AVG PUBLIC CISO TOTAL COMP

$686K

AVG PRIVATE CISO TOTAL COMP

KEY FINDING

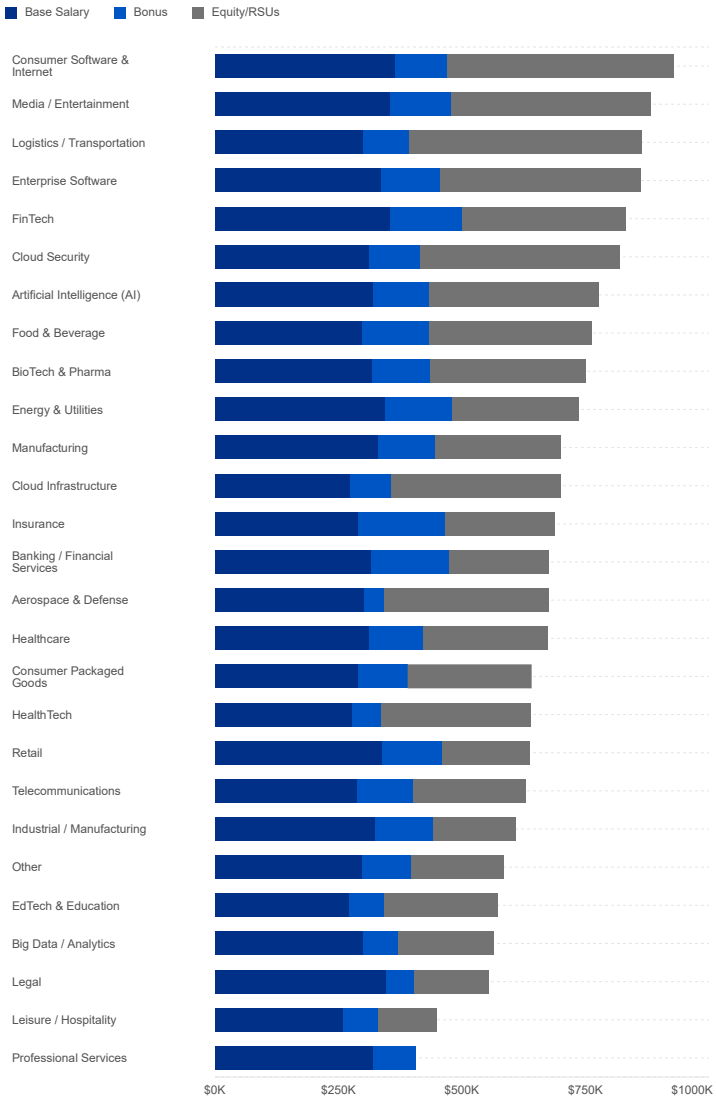
$814K **$686K**

Public company CISOs earn **$128K more** in total compensation, with equity driving the largest differential.

PUBLIC AVG | PRIVATE AVG

Industry Compensation Leaders

Total compensation varies significantly by industry vertical.



Consumer-facing software and media industries lead in total compensation, with equity packages accounting for up to 49% of total comp in top sectors.

** Industry category is self reported*

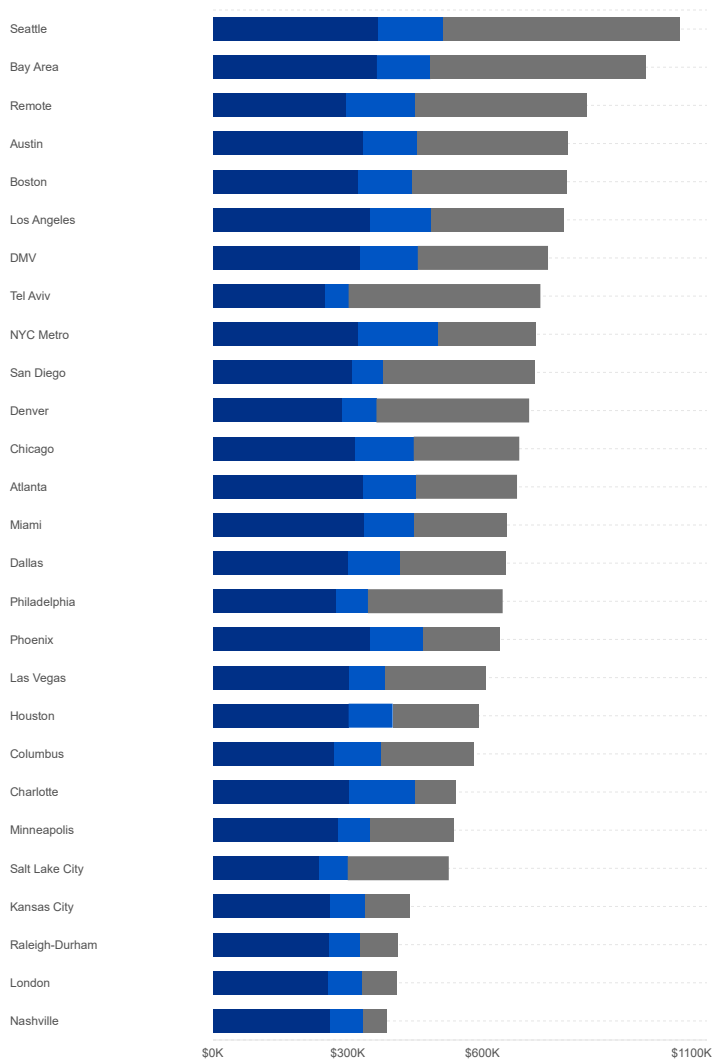
Consumer Software & Internet leads at $928K total compensation, driven by the highest equity packages ($458K avg). **Media/Entertainment** ($882K) and **Logistics/Transportation** ($864K) follow closely. Professional Services trails at $407K with minimal equity, reflecting partnership compensation models.

Geographic Insights

Location Premiums Persist Despite Remote Work Expansion

Base Salary | Bonus | Equity/RSUs

Compensation differences by location remain significant, with a 2.4x spread between top-paying markets such as Seattle and lower-cost metros like Kansas City.



Secondary markets show compressed arbitrage: Markets such as Austin, Denver, and Miami increasingly price near coastal compensation levels, indicating that geographic arbitrage advantages have narrowed as both companies and senior security talent have relocated to the same secondary hubs.

Employment Offer Bonus Trends

Signing bonus prevalence varies between public and private companies.

Public companies deploy larger signing bonuses to offset equity cliff risk and accelerate time-to-productivity.

PUBLIC COMPANIES

52%

offer signing bonuses

$184K

average bonus amount

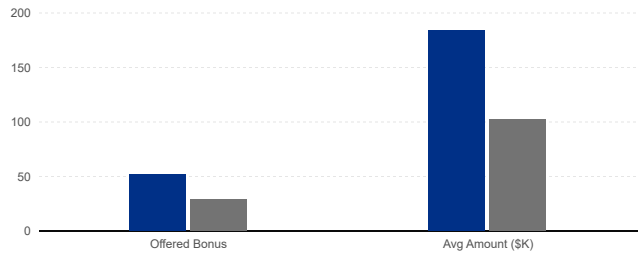
PRIVATE COMPANIES

29%

offer signing bonuses

$102K

average bonus amount



Public companies offer signing bonuses **79%** more frequently and at **80%** higher amounts than private counterparts, reflecting the need to offset equity cliff risk and accelerate candidate decisions.

SECTION 02

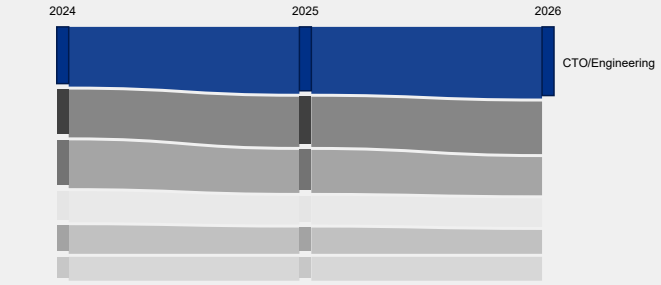
Reporting Structure Evolution

Security leadership has fundamentally realigned toward technical execution, with CTO and senior engineering leaders now representing the dominant reporting structure.

The CTO/Engineering Line Ascendancy

CTO and senior engineering leaders now represent 30-32% of CISO reporting relationships.

Private Companies | Public Companies



(30%)CIO (22%)CEO (16%)Other (12%)CFO (10%)General Counsel (10%)CISO Reports To

REPORTING LINES

CTO/Engineering CIO CEO CFO General Counsel Other

Private company CISOs show the strongest momentum toward CTO reporting with **+5%** year-over-year growth, signaling security's evolution from risk management to technical enablement.

+5%

YOY GROWTH IN PRIVATE CISOS REPORTING TO CTO/ENGINEERING

32%

CEO REPORTING AT COMPANIES <500 EMPLOYEES

63%

PUBLIC CISOS PRESENTING TO BOARD QUARTERLY

CIO reporting remains significant at 22% (private) and 34% (public), with steady but slower growth of +2% and +4% respectively. The CIO line reflects traditional IT-centric security models, while the accelerating CTO trend suggests organizations increasingly view security as integral to product development and engineering velocity.

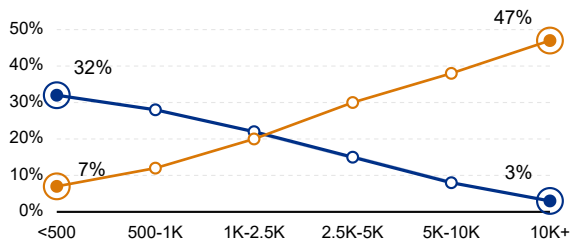
Company Size Dictates Access

Reporting to the CEO drops significantly as company size grows, while CIO reporting increases proportionally. Board reporting frequency also varies substantially between public and private companies.

At companies under 500 employees, 32% of CISOs report directly to the CEO. This collapses to just 3% at enterprises exceeding 10,000 employees.

REPORTING BY COMPANY SIZE

CEO and CIO reporting follows a predictable correlation with organizational scale

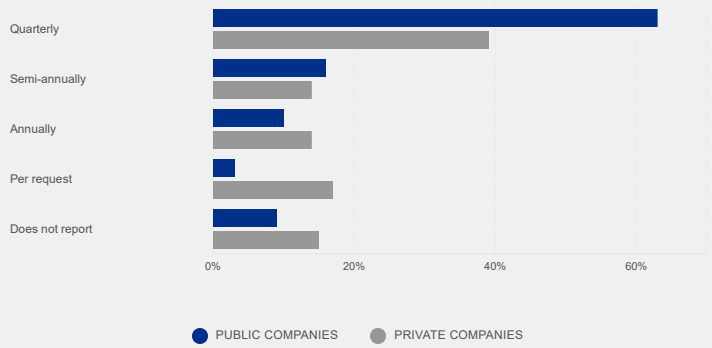


CEO
32% to 3%
-91% decline

CIO
7% to 47%
+571% increase

CISO REPORTING TO BOARD OF DIRECTORS

Reporting frequency by company type with year-over-year changes



63% of public vs **39% of private** companies report quarterly — a **24 percentage point gap**. Private companies show **-19% YoY decline** in board reporting overall.

63%	39%	9%	15%
PUBLIC QUARTERLY	PRIVATE QUARTERLY	PUBLIC DOES NOT REPORT	PRIVATE DOES NOT REPORT
+4% YoY	+3% YoY	-9% YoY	-19% YoY

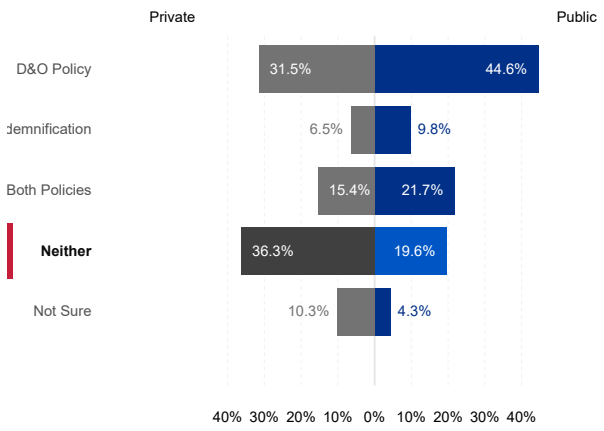
SECTION 03

CISO Liability Protection

Security leaders face significant personal risk with inadequate executive and personal liability coverage across both public and private sectors.

Executive Liability Coverage

D&O and indemnification policy adoption by company structure.



Key finding: Private company CISOs are **85% more likely** to have no executive liability protection compared to their public company peers.

36%
PRIVATE CISOS UNPROTECTED

20%
PUBLIC CISOS UNPROTECTED

Executive Liability Protection Gap: 36% of private and 20% of public CISOs lack coverage. S&P 500 executive protection benefits rose from 12% to 22.5% (2020–2024), per ISS-Corporate data reported by the Financial Times.

Personal Liability Insurance

Individual coverage rates reveal a widespread protection gap.

Personal Liability Insurance
Individual coverage rates for security executives by company structure

~75%
LACK PERSONAL COVERAGE

~74% of CISOs

lack personal liability insurance coverage, regardless of company structure

Privately Held Company — 74.7% unprotected

Publicly Traded Company — 73.4% unprotected

HAS COVERAGE
~26% of CISOs

NO COVERAGE
~74% of CISOs

Sector comparison: Personal liability coverage rates are nearly identical between public (26.6%) and private (25.3%) companies—a difference of only **1.3%**.

<2%

DIFFERENCE BETWEEN SECTORS

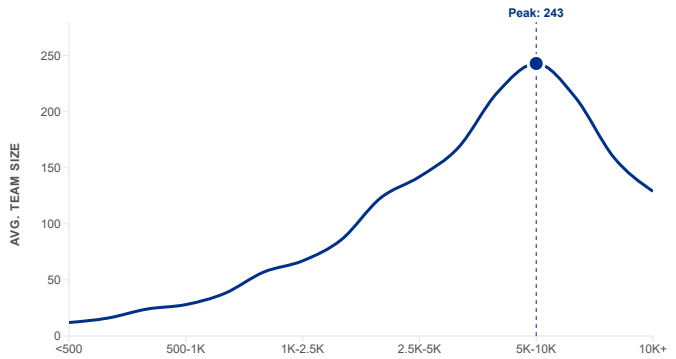
SECTION 04

Team Size Dynamics

Security team scaling follows a non-linear trajectory that peaks at upper mid-market scale before federation begins.

The Complexity Curve

Team size peaks at 5K-10K employees before declining due to federation.



Company Size — Drag to explore scaling phases

<500 | 500-1K | 1K-2.5K | 2.5K-5K | **5K-10K** | 10K+

5,000-10,000 EMPLOYEES

Peak Complexity

243 avg. security personnel

Maximum centralization achieved. Largest security teams at 243 personnel. Complexity outpaces informal controls.

<500	500-1K	1K-2.5K	2.5K-5K	5K-10K	10K+
12	28	67	142	243	129
Startup Mode	Early Scaling	Centralization	Scaling…	Peak…	Federation

243

PEAK SECURITY TEAM SIZE AT 5K-10K EMPLOYEE COMPANIES

-47%

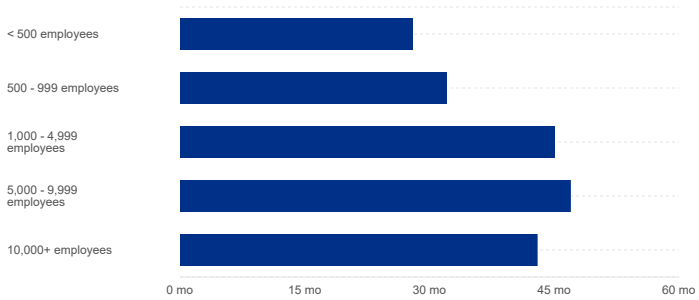
TEAM SIZE DECLINE AT 10K+ EMPLOYEES DUE TO FEDERATION

Key Insight: Security teams peak at 5K-10K employees (243 personnel) representing maximum centralization. Beyond 10K employees, teams contract 47% as organizations federate security responsibilities across platform teams and business units.

The “federation effect” becomes visible for organizations larger than 10,000 employees, where average team size contracts 47% to 129. Large enterprises distribute security responsibilities into other organizations including platform teams, IT functions, and enterprise risk (GRC). The CISO role transitions from large, self contained organization to governance, influence, and strategic oversight across federated security capabilities.

CISO Tenure by Company Size

Average tenure patterns reveal retention challenges at smaller organizations.



44 mo
PUBLIC COMPANY TENURE

36 mo
PRIVATE COMPANY TENURE

CISOs at sub-500 employee companies average just **28 months** tenure (40% shorter than the 47-month average at mid-market firms). The role at this stage is often under-resourced, under-scoped, and positioned as a checkbox rather than a function.

SECTION 05

CISO Functional Responsibilities

Security leadership encompasses a diverse portfolio of direct responsibilities from universal operational functions to emerging AI governance revealing where accountability is concentrated and where critical gaps persist.

Direct Responsibility Landscape

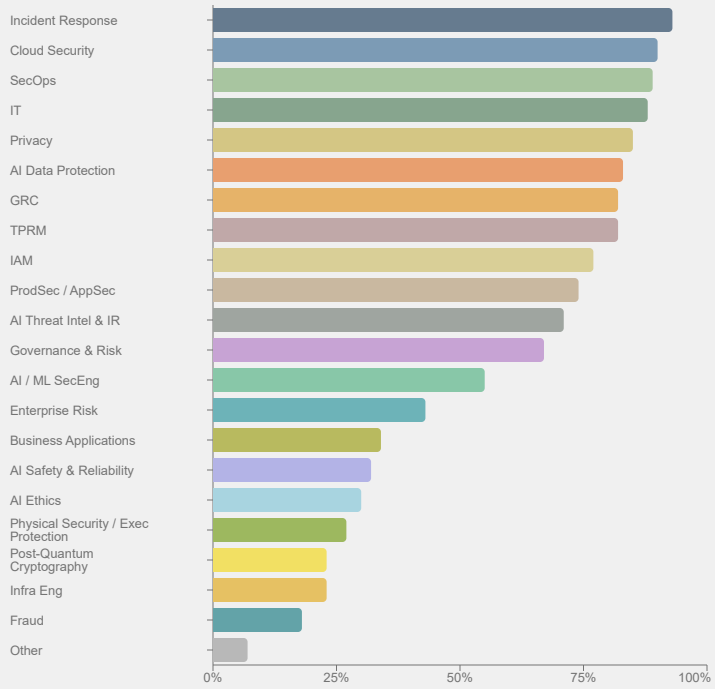
Percentage of North American CISOs with direct oversight of each security function.

93%
CISOS OWN INCIDENT RESPONSE

12
AVERAGE FUNCTIONS PER CISO

88%
CISO RESPONSIBLE FOR IT

74%
CISO RESPONSIBLE FOR PRODUCT/APPLICATION SECURITY



The data reveals three distinct clusters: **universal operational functions** (Incident Response, Cloud Security, SecOps at 88-93%), **converging risk functions** (Privacy, GRC, TPRM at 82-85%), and **fragmented emerging functions** (AI Ethics, Post-Quantum Cryptography, Fraud at 18-30%). This fragmentation in emerging areas suggests either unclear ownership models or security functions still maturing into CISO portfolios. This gap between technical control and governance oversight creates the AI leadership vacuum explored in the next section.

SECTION 06

AI Governance and Risk Management

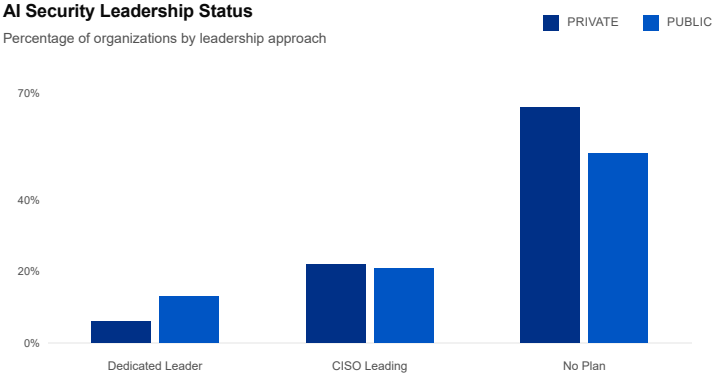
Organizations face a critical gap between AI adoption velocity and security preparedness, with structural vulnerabilities across governance, technical capability, and executive protection.

AI Security Leadership Vacuum

Only 6% of private and 13% of public companies have dedicated AI security leaders.

AI Security Leadership Status

Percentage of organizations by leadership approach



6%

PRIVATE COMPANIES WITH DEDICATED AI SECURITY LEADERS

84%

SECURITY LEADERS LACK FULL CONFIDENCE IN TECHNICAL ASSESSMENT

Leadership Vacuum Identified

Only **6%** of private and **13%** of public companies have dedicated AI security leaders. Two-thirds of private organizations have no AI security leadership strategy.

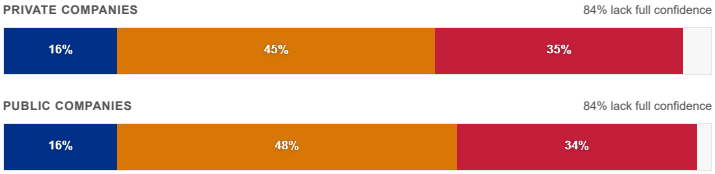
DEDICATED LEADER	CISO LEADING	NO PLAN
6% Priv 13% Pub	22% Priv 21% Pub	66% Priv 53% Pub

Technical Assessment Confidence Gap

CISOs lack confidence in their ability to evaluate technical talent.

Technical Assessment Capability

Confidence in recruiting team's ability to assess technical depth

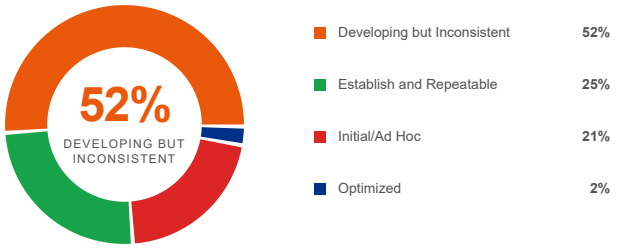


Very Confident	Somewhat Confident	Not Confident
Pvt: 16% | Pub: 16%	Pvt: 45% | Pub: 48%	Pvt: 35% | Pub: 34%

Only **16%** of CISOs express high confidence. The majority report "somewhat confident" (45-48%), while 34-35% admit lacking confidence entirely. When organizations can't assess technical depth, they default to proxies like credentials and brand names. This potentially results in growing headcount without growing capability and increasing risk with each hiring cycle.

AI Governance and Risk Management Maturity

Shadow AI and accountability definition top the list of governance concerns.



73%
AD HOC & INCONSISTENT

73% lack mature AI governance (52% Developing but inconsistent + 21% Initial / ad hoc), with only 25% achieving Established and Repeatable processes and just 2% reaching Optimized maturity.

52%
DEVELOPING BUT INCONSISTENT

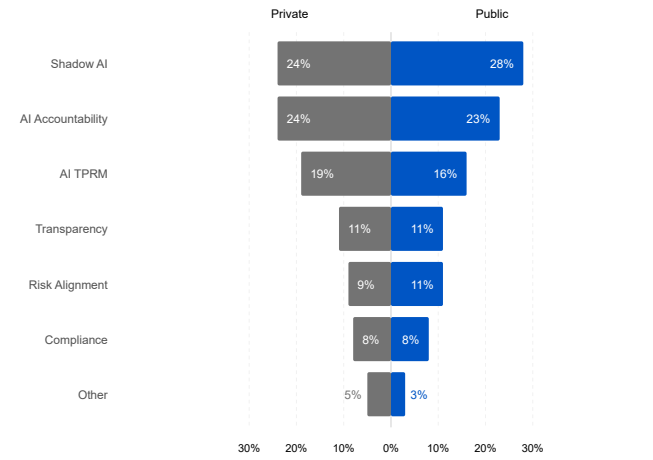
Only 25% of organizations report "established and repeatable" AI governance processes with 66% of private and 53% of public companies having no plans to hire dedicated AI security leadership.

AI Challenges and Concerns

AI security spending averages anticipated spend of 7% of total security budget

GREATEST AI GOVERNANCE CHALLENGE

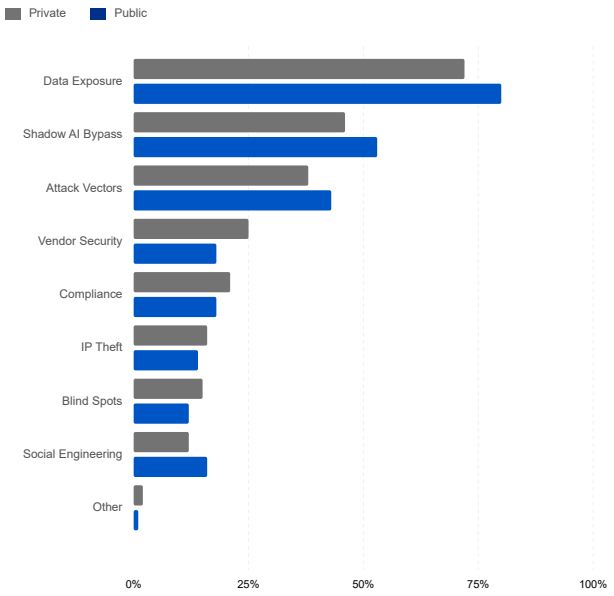
Comparing governance and risk management challenges between private and public companies



Key finding: Shadow AI and accountability definition are the **top two challenges** for both company types, accounting for 48-51% of governance concerns.

GREATEST CONCERNS REGARDING AI TOOLS USE

Security concerns about AI tool adoption in private vs public companies



Key finding: Public companies show **8% higher concern** about data exposure and privacy breaches, reflecting increased regulatory scrutiny and stakeholder expectations.

75%

CITE DATA EXPOSURE AS TOP AI RISK

Data Exposure Dominates AI Concerns 75% of CISOs cite data exposure/privacy breaches as the top AI risk, followed by shadow AI bypassing controls (49%).

AI GOVERNANCE FRAMEWORKS IN USE OR PLANNED

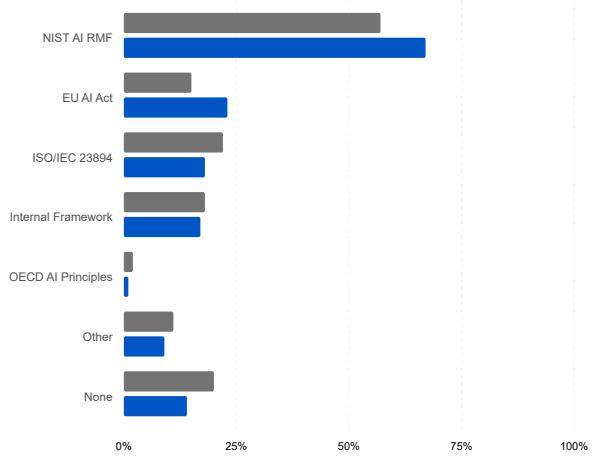
The NIST AI RMF has emerged as the leading framework

Private Public

67%

PUBLIC COMPANIES USING NIST AI RMF

NIST AI Framework established as clear market preference over alternatives, 3x more likely.



Key finding: NIST AI RMF dominates with **57-67% adoption**, while 14-20% of organizations have no AI governance framework in place.

SECTION 07

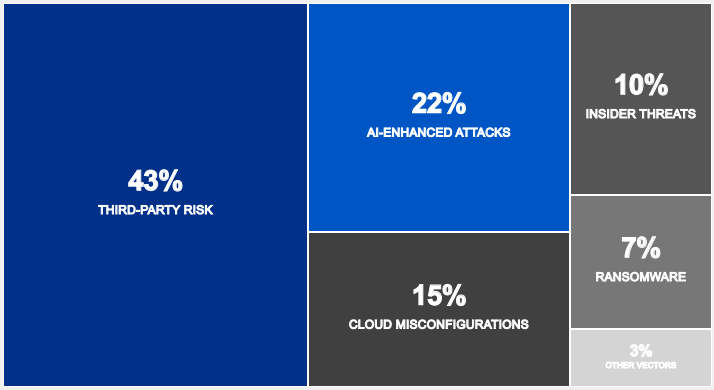
Threat Landscape 2026

Third-party risk dominates security priorities, with AI-enhanced attacks and cloud misconfigurations completing the top three concerns.

Attack Vector Security Priorities

Top security priorities for 2026 ranked by CISO concern.

Third-party Risk **43%** AI-enhanced Attacks **22%** Cloud Misconfigurations **15%**
Insider Threats **10%** Ransomware **7%** Other Vectors **3%**



Third-party risk dominates 2026 priorities at 43%, nearly double AI-enhanced attacks (22%). This reflects growing supply chain complexity and recent high-profile vendor breaches.

43%

THIRD-PARTY RISK AS #1 SECURITY PRIORITY

Third-party risk ranks as the overwhelming #1 priority. Modernize TPRM programs with continuous monitoring and tiered risk frameworks.

Budget Justification Measures

How CISOs justify security budget requirements to leadership.

1 Business Impact **69%**

2 Attack Surface Expansion **58%**

Business Impact Overtakes Compliance 69% justify security budgets via business impact versus 49% through compliance avoidance, marking shift from "cost of doing business" to "enabler of business outcomes."

3	Compliance and Regulatory Mandates	49%
4	Financial Metrics and ROI	42%
5	Revenue Percentage Allocation	10%

Only 10% use percentage-of-revenue models, indicating CISO sophistication in tying security to business value rather than arbitrary formulas.

69%	58%	49%
BUSINESS IMPACT	ATTACK SURFACE	COMPLIANCE

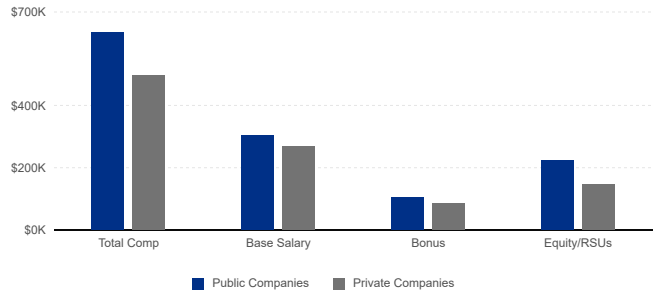
SECTION 08

NextGen Security Leaders

Deputy CISOs, Heads of Security Engineering, and domain-specific Directors represent the execution layer bridging strategy with hands-on program delivery.

Compensation Dynamics

NextGen compensation growth is outpacing CISO increases, signaling execution-layer talent scarcity.



37
AVERAGE DIRECT REPORTS

Key Insight: The larger YoY compensation growth in NextGen roles compared to CISOs signals a fundamental market shift: execution capability now commands a higher premium than strategic oversight. As the CISO role increasingly emphasizes risk communication, board presentations, and stakeholder management, the market is bidding up the technical leaders who architect, build, and operate security programs.

Employment Incentives

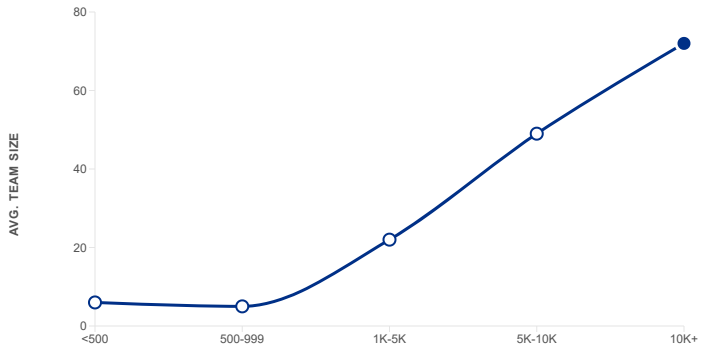
Signing bonus prevalence mirrors CISO patterns—public companies deploy larger bonuses to offset equity cliff risk.

PUBLIC COMPANIES	PRIVATE COMPANIES
65%	**53%**
Offer signing bonuses	Offer signing bonuses
$73K avg	**$48K avg**

Private companies offer 53% of NextGen roles with signing bonuses versus 65% for public companies, with public bonuses 53% higher ($73K vs $48K). This suggests private companies using cash incentives to compete with public company stability.

Span of Control

NextGen security leaders manage teams that scale dramatically with company size, from lean startup teams to large enterprise operations.



Company Size

Drag to explore team scaling

<500 | 500-999 | 1K-5K | 5K-10K | **10K+**

10,000+ EMPLOYEES

Company Size: 10K+

72 avg. direct reports

At enterprise scale, NextGen security leaders manage the largest teams, reflecting mature security programs with specialized roles.

<500	500-999	1K-5K	5K-10K	10K+
6	5	22	49	72
Under 500	500-999	1,000-4,999	5,000-9,999	10,000+

Cloud Security and AppSec leaders tend toward smaller, highly technical teams, while GRC and Security Operations leaders manage larger operational groups.

SECTION 09

International CISO Landscape

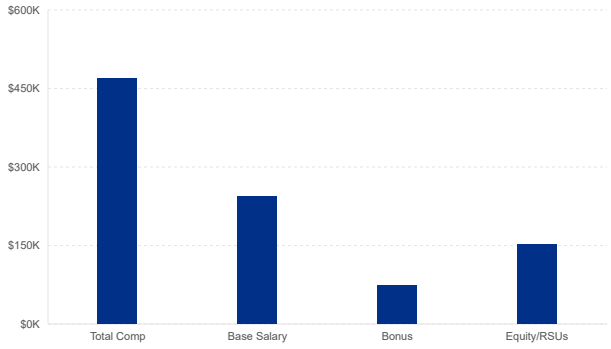
European and international CISOs operate in distinctly different contexts; 32% lower compensation, broader regulatory responsibilities, and unique team scaling patterns shaped by GDPR and centralized governance models.

Compensation Gap: International vs. North America

International CISOs earn $469K total compensation which is 32% below the North American average of $750K.

INTERNATIONAL CISO COMPENSATION BREAKDOWN

Total compensation analysis by component



$469K
INT'L AVG TOTAL COMP

$750K
NORTH AMERICA AVG

-32%
COMPENSATION GAP

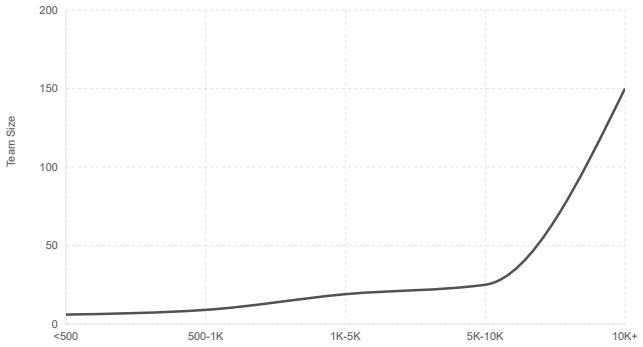
Lower equity prevalence and regional market differences drive the compensation differential. Base

International CISOs earn **$469K** in total compensation, composed of **$243K** base salary (52%), **$74K** bonus (16%), and **$152K** in equity (32%). Equity represents nearly one-third of total compensation, highlighting the importance of long-term incentive alignment.

$469K	$243K	$74K	$152K
TOTAL COMPENSATION	BASE SALARY	BONUS	EQUITY/RSUS

salaries show smaller variance ($243K vs $364K North America average).

Team Scaling Patterns



6	19	25	150
STARTUP (<500)	MID-MARKET (1K-5K)	GROWTH (5K-10K)	ENTERPRISE (10K+)

150
INT'L TEAM SIZE AT 10K+ EMPLOYEES

129
NORTH AMERICA 10K+

+16%
ENTERPRISE SCALE DIFFERENCE

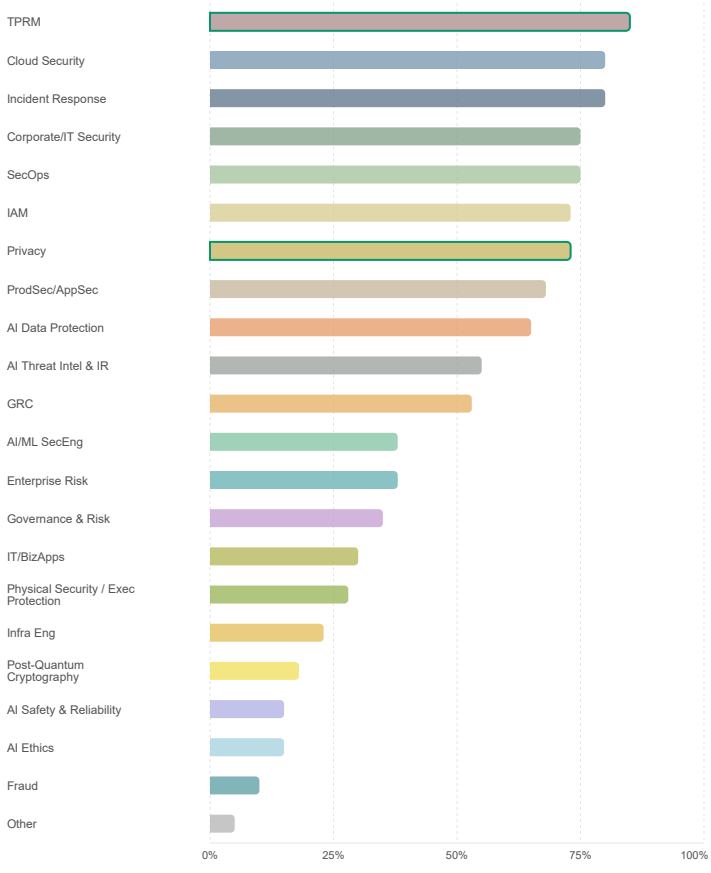
Higher enterprise team sizes suggest less federation in international markets, with centralized security models persisting longer as companies scale.

Functional Responsibilities: Regulatory-Driven Priorities

International CISOs oversee an average of 10 functions (vs 12 in NA) with significantly higher ownership of TPRM and Privacy.

FUNCTIONS UNDER INTERNATIONAL CISO DIRECT RESPONSIBILITY

All 22 functions showing regulatory-driven priorities: TPRM (85%), Privacy (73%)



85%
TPRM OWNERSHIP

vs 41% in North America. Largest gap (+44pp) driven by GDPR, NIS2, and DORA regulatory emphasis

73%
PRIVACY OWNERSHIP

vs 58% in North America (+15pp). GDPR enforcement and DPO reporting structures

10
AVG FUNCTIONS PER CISO

TPRM (THIRD-PARTY RISK)

85% international vs 41% NA

+44pp gap driven by GDPR, NIS2, and DORA regulatory emphasis

PRIVACY

73% international vs 58% NA

+15pp gap reflecting GDPR enforcement and DPO reporting structures

10	12	85%	73%
AVG FUNCTIONS PER CISO	NORTH AMERICA AVG	TPRM OWNERSHIP	PRIVACY OWNERSHIP

SECTION 10

Strategic Imperatives for 2026

Six critical actions for security leaders navigating compensation, governance, and organizational challenges. Click any imperative to explore implementation details and related data points.

6	3	3	2026
STRATEGIC IMPERATIVES	CRITICAL PRIORITY	HIGH PRIORITY	TARGET YEAR

ROADMAP PROGRESS

1. Close the Compensatio…
2. Navigate CTO-Line Rep…
3. Mature AI Governance
4. Secure Liability Protecti…
5. Manage Third-Party Risk
6. Develop NextGen Pipel…

1 CRITICAL

Close the Compensation Gap

The $128K public-private delta creates retention risk for private company CISOs.

$128K PUBLIC-PRIVATE COMPENSATION GAP

2 HIGH

Navigate CTO-Line Reporting

With 30-32% of CISOs reporting to CTOs, security must demonstrate technical enablement value.

30-32% CTO/ENGINEERING REPORTING DOMINANCE

3 CRITICAL

Mature AI Governance

95%+ organizations lack mature AI governance frameworks despite accelerating adoption.

2% OPTIMIZED AI GOVERNANCE

4 CRITICAL

Secure Liability Protection

36% of private company CISOs operate without any executive liability protection.

36% PRIVATE CISOS WITHOUT PROTECTION

5 HIGH

Manage Third-Party Risk

Third-party risk ranks as the #1 security priority for 43% of respondents.

43% THIRD-PARTY RISK AS #1 PRIORITY

6 HIGH

Develop NextGen Pipeline

NextGen compensation growth outpacing CISO increases signals execution-layer talent scarcity.

YOY+ NEXTGEN COMP OUTPACING CISO GROWTH

KEY INSIGHT

Organizations face converging pressures: compensation inflation, AI governance immaturity, liability exposure gaps, and third-party risk concentration. Success requires parallel investment in NextGen talent development and structural security program maturity.

2026 Global CISO Leadership Report

Data collected Q4 2025 – Q1 2026. All compensation figures in USD.