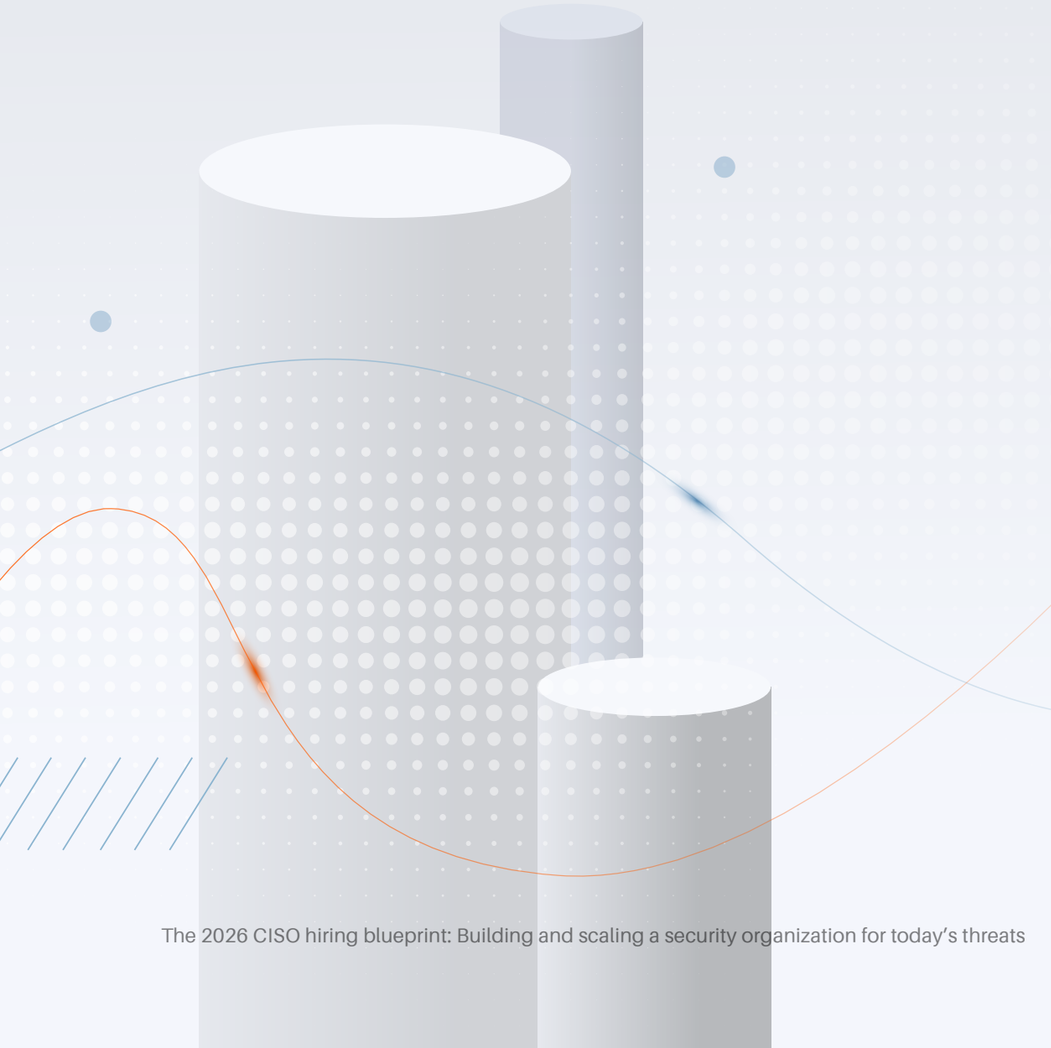
The CISO Hiring Blueprint:

How to Hire, Structure, and Support Cyber Leadership in 2026

Riviera
PARTNERS

Table of contents



A bottom line issue for boardrooms

In 2025 alone, cybercrime cost the global economy approximately

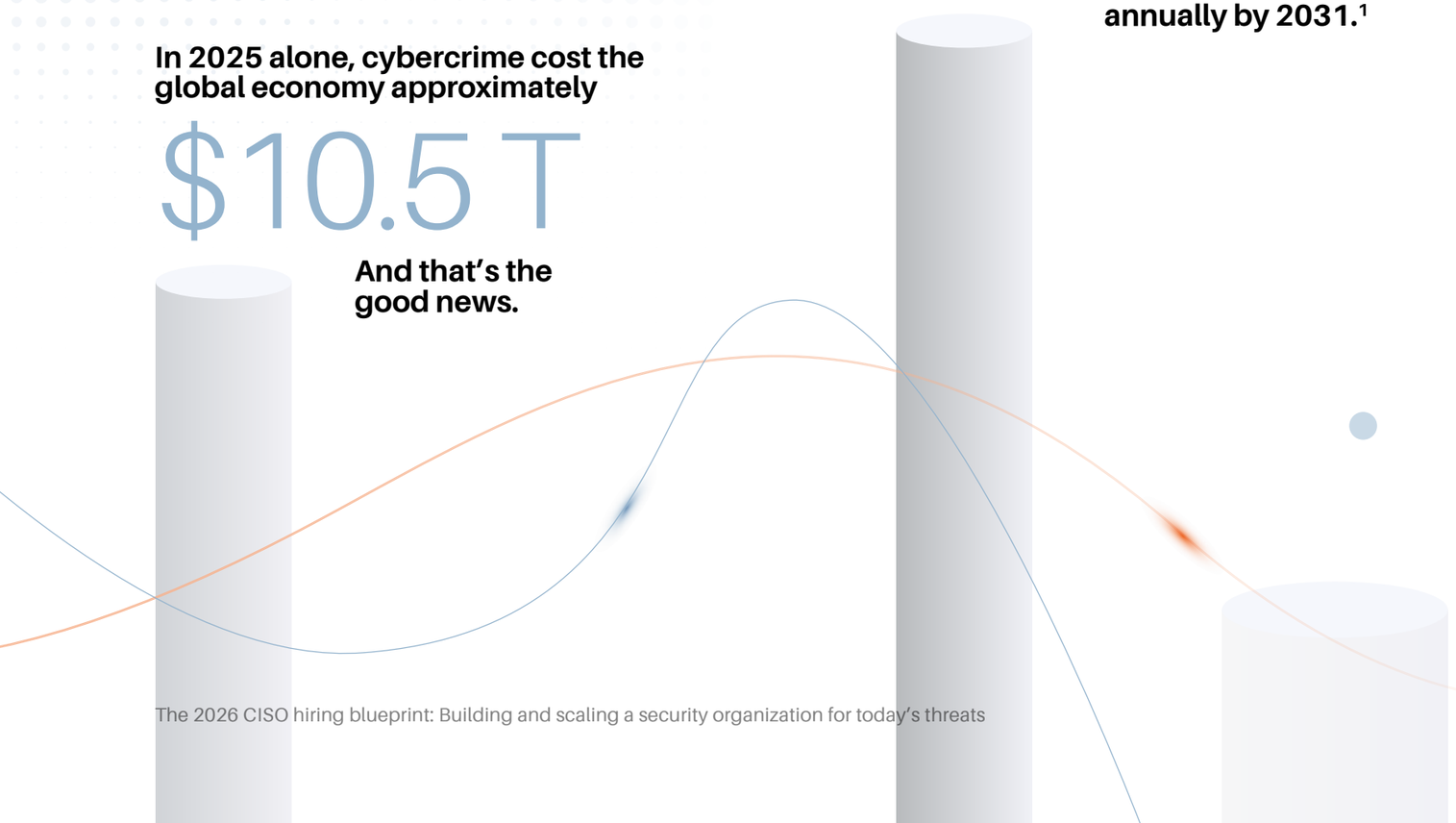
$10.5 T

And that's the good news.

The bad news is that businesses can expect the cost to rise to

$12.2 T

annually by 2031.[1]



For today's CEOs and their boards, cybersecurity is now as much a bottom line issue as it is a technical one. As a result, many organizations are beginning to prioritize and empower the Chief Information Security Officer (CISO) role. Today's CISOs are expected to think beyond protecting the perimeter to protecting their organization's reputation and revenue.

This guide is designed to give organizations the blueprint they need to find, hire, and support the right cybersecurity leaders to meet today's environment. With real-world insight into the demands of the position backed by real market data on compensation and proven organizational structures, you'll learn how to keep your organization ahead of threats in 2026 and beyond.

[1] Cybercrime Magazine, Cybercrime to Cost the World $12.2 Trillion Annually by 2031.

Cyber risk = enterprise risk

Thanks to a proliferation of high-profile attacks, cyber risk is now one of the board's top concerns. They now realize that an attack is not a matter of if, but when, shifting the cyber risk conversation from 'Are we protected?' to 'Are we prepared?' For many organizations, the answer is no.

And with the rise of AI, the outlook only looks more dire. Organizations are deploying AI across products, operations, and workflows as fast as possible, creating new attack surfaces that few organizations have experience defending. At the same time, attackers are using AI to scale attacks, automate reconnaissance, and adapt to defense strategies faster.[2]

AI is already worrying enterprise security teams:

73%

of leaders say AI-powered threats have significantly impacted their organizations,

while

92%

say they have required significant upgrades to their defenses.

Beyond AI-enabled threats, ransomware and extortion campaigns are now a fact of life, with 93% of businesses saying they've experienced at least one attack within the last 24 months.[3]

And even if your organization runs a best-in-class security operation, today's reliance on cloud platforms, AI vendors, and interconnected ecosystems means third-party risk is now inseparable from your internal security posture.

Whether it hits your in-house servers or takes down a critical partner, a large-scale attack can now devastate finances, operations, and reputations, transforming what used to be an IT headache into an enterprise concern involving legal, communications, and executive leadership.

Taken together, these shifts define the new baseline for 2026: faster attack cycles, multi-front incidents, and heavier governance expectations. For business leaders and their boards, it's no longer a question of whether their organization has the right tools for the job, but the right person.

[2] Darktrace, The State of AI Cybersecurity 2026
[3] Morphisec, Ransomware Reality Check

Why the CISO role can’t wait

For years, companies have treated the CISO hire as a milestone that’s reached when the security needs of the organization outgrow the capabilities of IT. But today, the CISO role is as important as the CIO, CFO, or COO, and should be considered a foundational leadership role.

High-performing growth-stage and middle-market organizations are now hiring CISOs earlier in their lifecycle, often for the first time. For companies looking toward the 2027 IPO window, now is the time to establish their CISO function so their governance and documented risk oversight are in place before public filing.

Meanwhile, organizations working in regulated industries have discovered that their security posture is directly tied to revenue. Detailed security questionnaires, third-party audits, and formal attestations are now standard components of the buying process, which requires a CISO to oversee responses, validate controls, and credibly represent the company’s risk posture to buyers and regulators alike.

As governance scrutiny increases, nearly half of organizations anticipate board-driven changes in executive responsibilities.[4] For many, the conclusion is that cybersecurity can no longer be left to IT. They now require a dedicated security leader who is directly accountable to the executive team and the board.

[4] Riviera Partners, The Future of Tech Leadership Survey Report 2025.

The modern CISO mandate by company stage

Not all CISO mandates are created equal. Here's what organizations expect from their security leadership across key company stages.

VC-backed firms

These companies have a need for speed, often hiring their first CISO while still fine-tuning product-market fit or scaling the business. These organizations require pragmatic, hands-on builders who can design foundational security architecture, implement core controls, and partner closely with engineering without slowing innovation.

PE-backed firms

These companies are just as focused on protecting the bottom line as they are their attack surface. They look for CISOs who can formalize governance, strengthen third-party risk oversight, rationalize tooling spend, and demonstrate a measurable reduction in exposure. In addition, they need leaders who can support M&A diligence and post-acquisition integration to ensure security risk is understood, priced, and properly managed across the portfolio.

Public companies

Incident response is as much a governance and disclosure undertaking as it is a technical one, requiring CISOs who can focus on disclosure discipline, regulatory alignment, and audit readiness. Security leaders for these organizations need to be comfortable working within complex global environments, overseeing mature security teams, and engaging directly with regulators, the board, and investors. At the same time, they're expected to leverage AI and automation to improve detection and response without increasing headcount.

Regardless of size or stage, high-performing companies require CISOs with a consistent set of leadership traits:

- Strong technical judgement: While they won't personally configure every control, the CISO should be able to quickly assess architectural trade-offs, evaluate vendor risk, and use AI to augment analysis and prioritize response..
- Business operator mindset: Modern CISOs are evaluated as much on security outcomes as they are on the impact security has on revenue, profitability, and the customer experience. .
- Board and executive communication: The CISO must be able to translate technical exposure into enterprise risk so they can adequately brief boards and articulate risk acceptance decisions in clear, defensible terms.
- Organizational builder: An effective CISO can build the right mix of governance, architecture, detection, and response capabilities while creating a culture that balances vigilance with cross-functional collaboration.
- Crisis leadership: When a crisis breaks out, the CISO is the point person coordinating legal, communications, operations, and the executive team. Calm decision-making, structured escalation, and credibility under pressure is essential.

CISO success metrics

Here are a few ways organizations can monitor CISO performance:

- Outcome metrics, such as a measurable reduction in risk exposure and improved organizational resilience.
- Operating metrics, such as remediation velocity, detection and response readiness, and the maturity of identity and access controls.
- Business enablement metrics, such as audit readiness, reduced sales friction tied to security posture, and faster speed entering or expanding into regulated markets.

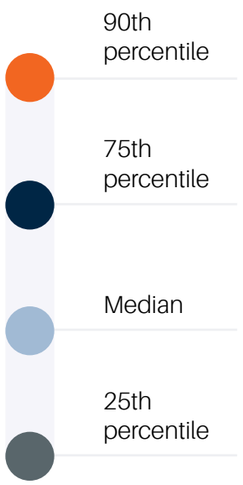
CISO compensation and incentives by the numbers

Security leadership compensation now reflects both competitive demand and business consequences, with the role increasingly benchmarked against other top executives instead of purely technical leaders.

Demand for CISOs has also surged to the busiest level seen in years. Many companies that historically delayed or avoided hiring a dedicated security leader are now entering the market at the same time, creating urgency, higher price tags, and a sharper need to understand true market compensation for the role.

For top CISOs, compensation signals how seriously–or not–an organization treats security oversight, accountability, and operational resilience. Based on our extensive, real-world placements of CISOs in 2025, here's what you can expect to pay your next cyber leader.

Chart legend



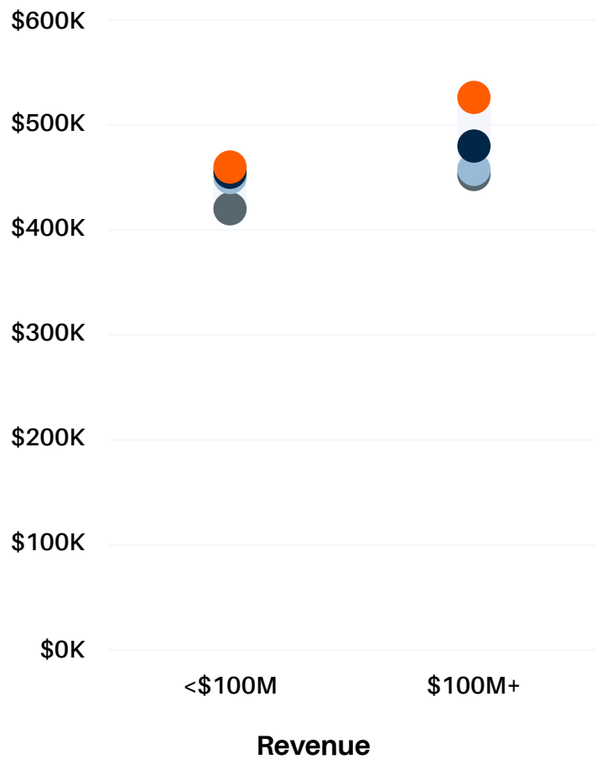
The charts included in this report present a comprehensive overview of:

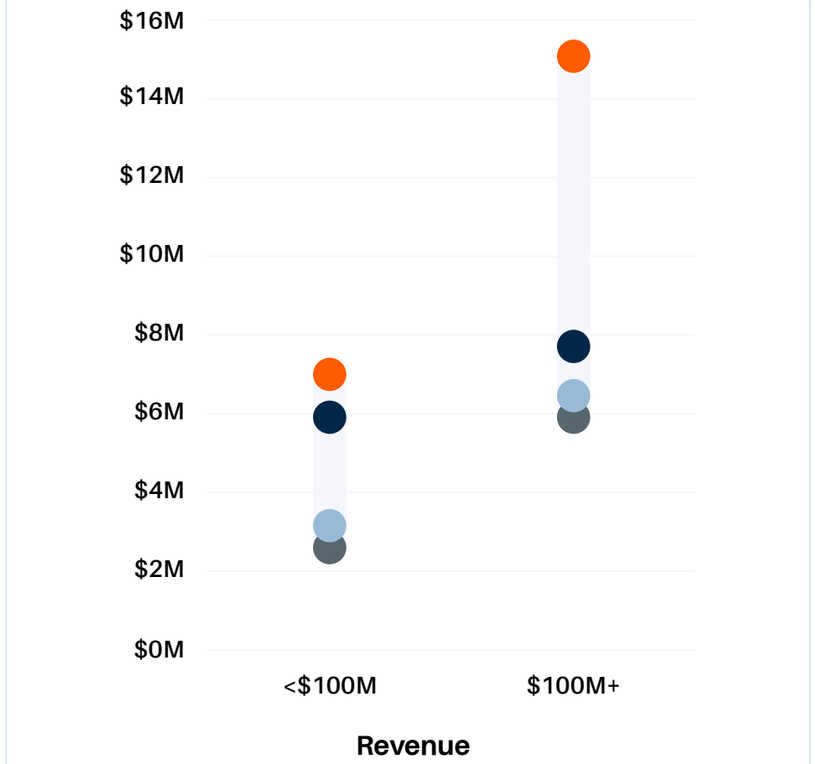
- Total annual cash compensation, inclusive of annual salary and incentive bonuses (sign-on bonuses are excluded)
- Frequency of offers that include an annual bonus, and the percent the annual bonus represents of the annual salary
- Frequency of offers that include a sign-on bonus, and the percent the sign-on bonus represents of the annual salary
- For VC and Public, the equity grant is based on companies of all types and classifications and typically reflects estimated gross initial grant (non-annualized); for PE, equity is typically based on estimated gross exit value

Questions? Please reach out for more specifics.
Contact@rivierapartners.com

IT/CYBERSECURITY

US Venture Capital: by revenue





Legend

- 90th Percentile
- 75th Percentile
- Median
- 25th Percentile

NOTE:

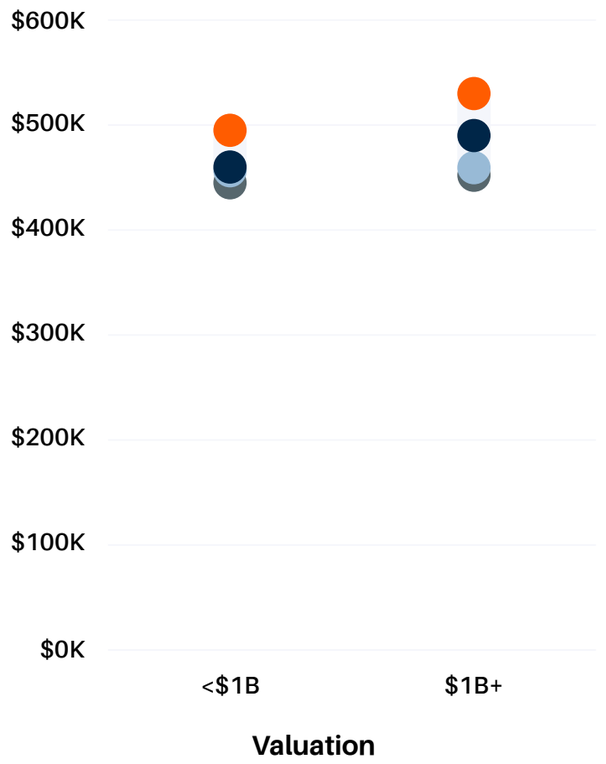
Total cash compensation is comprised of annual salary and on-target bonuses, calculated on an annual basis.

Sign-on and relocation bonuses are not included in total annual cash compensation bonus.

Equity grant is based on companies of all types and classifications and typically reflects estimated gross initial grant (non-annualized).

IT/CYBERSECURITY

US Venture Capital: by valuation



Legend

- 90th Percentile
- 75th Percentile
- Median
- 25th Percentile

NOTE:

Total cash compensation is comprised of annual salary and on-target bonuses, calculated on an annual basis.

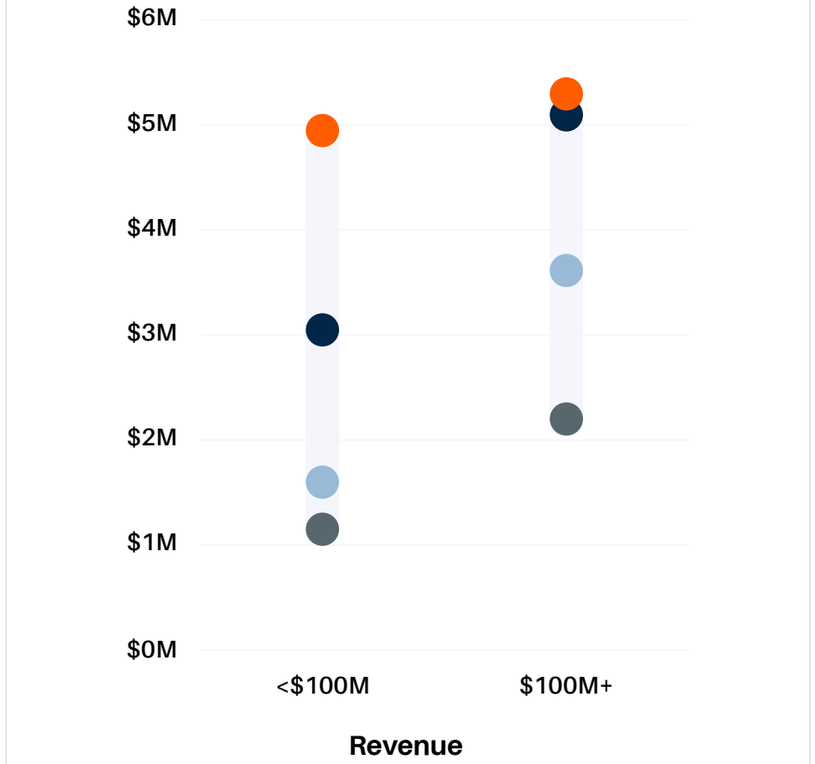
Sign-on and relocation bonuses are not included in total annual cash compensation bonus.

Equity grant is based on companies of all types and classifications and typically reflects estimated gross initial grant (non-annualized).

Companies are segmented by valuation when available, otherwise series used as proxy.

IT/CYBERSECURITY

US Venture Capital: by revenue



Legend

- 90th Percentile
- 75th Percentile
- Median
- 25th Percentile

NOTE:

Total cash compensation is comprised of annual salary and on-target bonuses, calculated on an annual basis.

Sign-on and relocation bonuses are not included in total annual cash compensation bonus.

Equity grant is based on companies of all types and classifications and typically reflects estimated gross initial grant (non-annualized).

IT/CYBERSECURITY

US Venture Capital: by valuation

Legend

- 90th Percentile
- 75th Percentile
- Median
- 25th Percentile

NOTE:

Total cash compensation is comprised of annual salary and on-target bonuses, calculated on an annual basis.

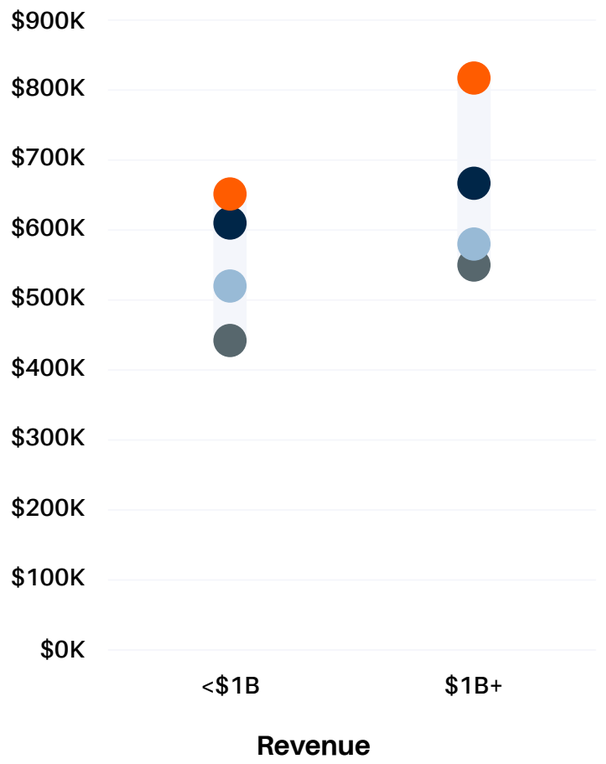
Sign-on and relocation bonuses are not included in total annual cash compensation bonus.

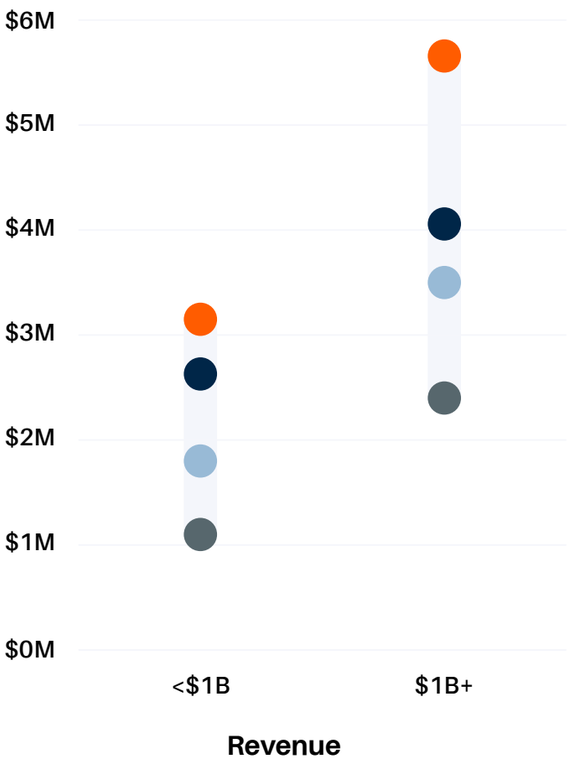
Equity grant is based on companies of all types and classifications and typically reflects estimated gross initial grant (non-annualized).

Companies are segmented by valuation when available, otherwise series used as proxy.

IT/CYBERSECURITY

US Private-Equity backed





Legend

- 90th Percentile
- 75th Percentile
- Median
- 25th Percentile

NOTE:

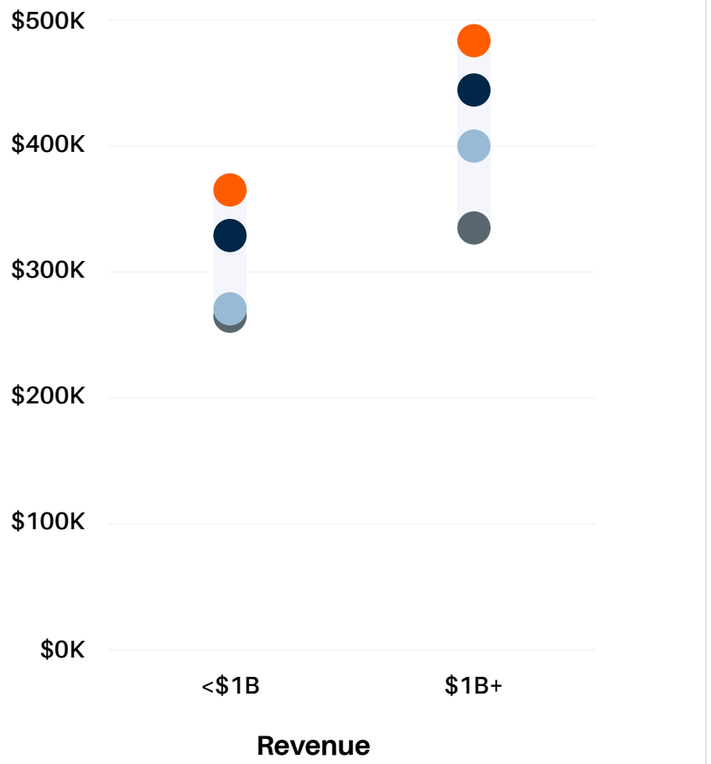
Total cash compensation is comprised of annual salary and on-target bonuses, calculated on an annual basis.

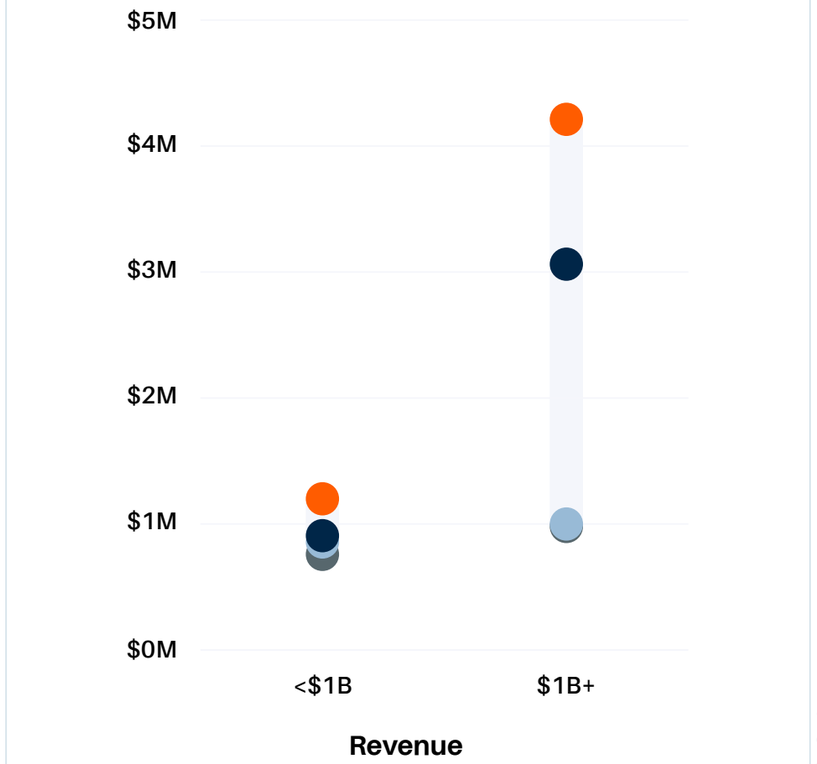
Sign-on and relocation bonuses are not included in total annual cash compensation bonus.

Equity grant is based on companies of all types and classifications and typically reflects estimated gross exit value (non-annualized).

IT/CYBERSECURITY

US Private-Equity backed





Legend

- 90th Percentile
- 75th Percentile
- Median
- 25th Percentile

NOTE:

Total cash compensation is comprised of annual salary and on-target bonuses, calculated on an annual basis.

Sign-on and relocation bonuses are not included in total annual cash compensation bonus.

Equity grant is based on companies of all types and classifications and typically reflects estimated gross exit value (non-annualized).

IT/CYBERSECURITY

US Public

Legend

- 90th Percentile
- 75th Percentile
- Median
- 25th Percentile

NOTE:

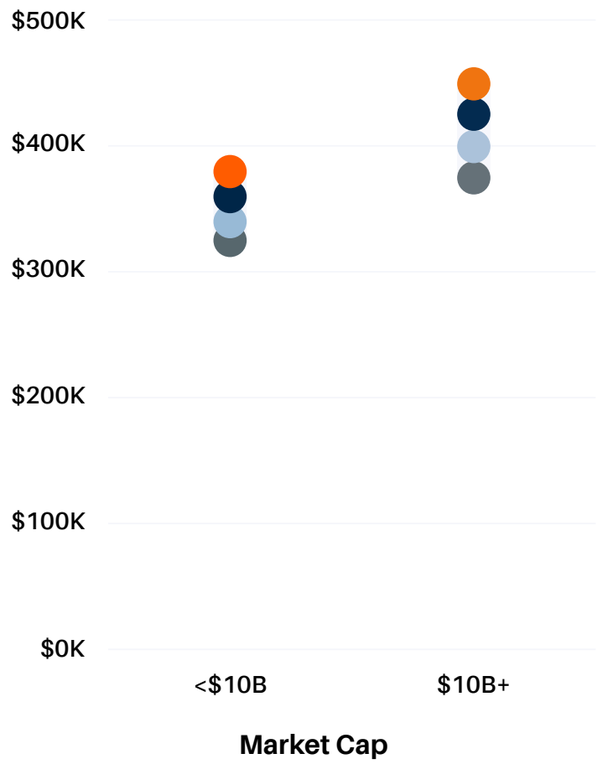
Total cash compensation is comprised of annual salary and on-target bonuses, calculated on an annual basis.

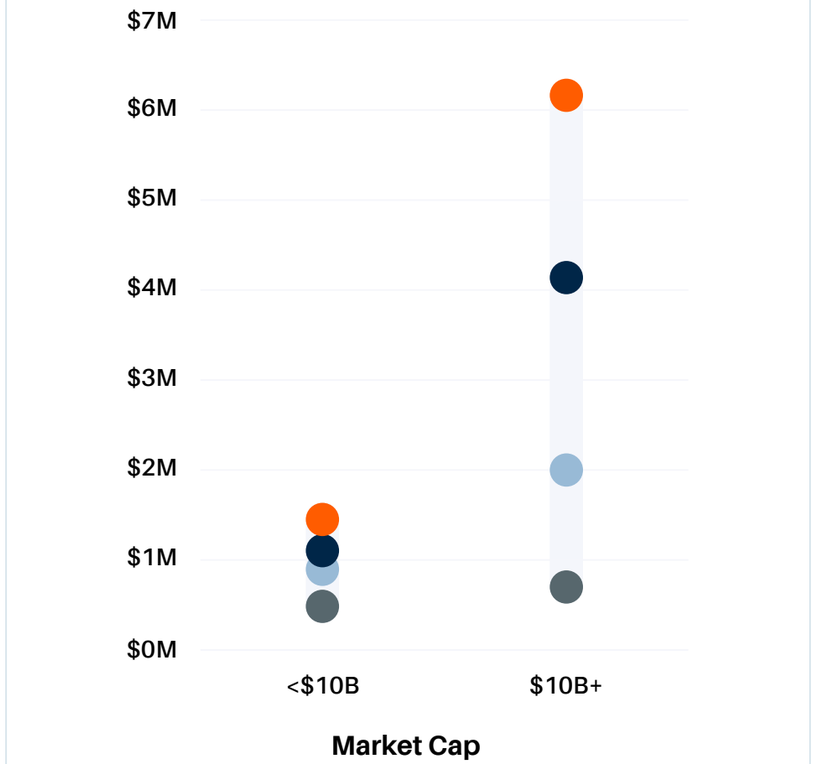
Sign-on and relocation bonuses are not included in total annual cash compensation bonus.

Equity grant is based on companies of all types and classifications and typically reflects estimated gross initial grant (non-annualized).

IT/CYBERSECURITY

US Public





Legend

- 90th Percentile
- 75th Percentile
- Median
- 25th Percentile

NOTE:

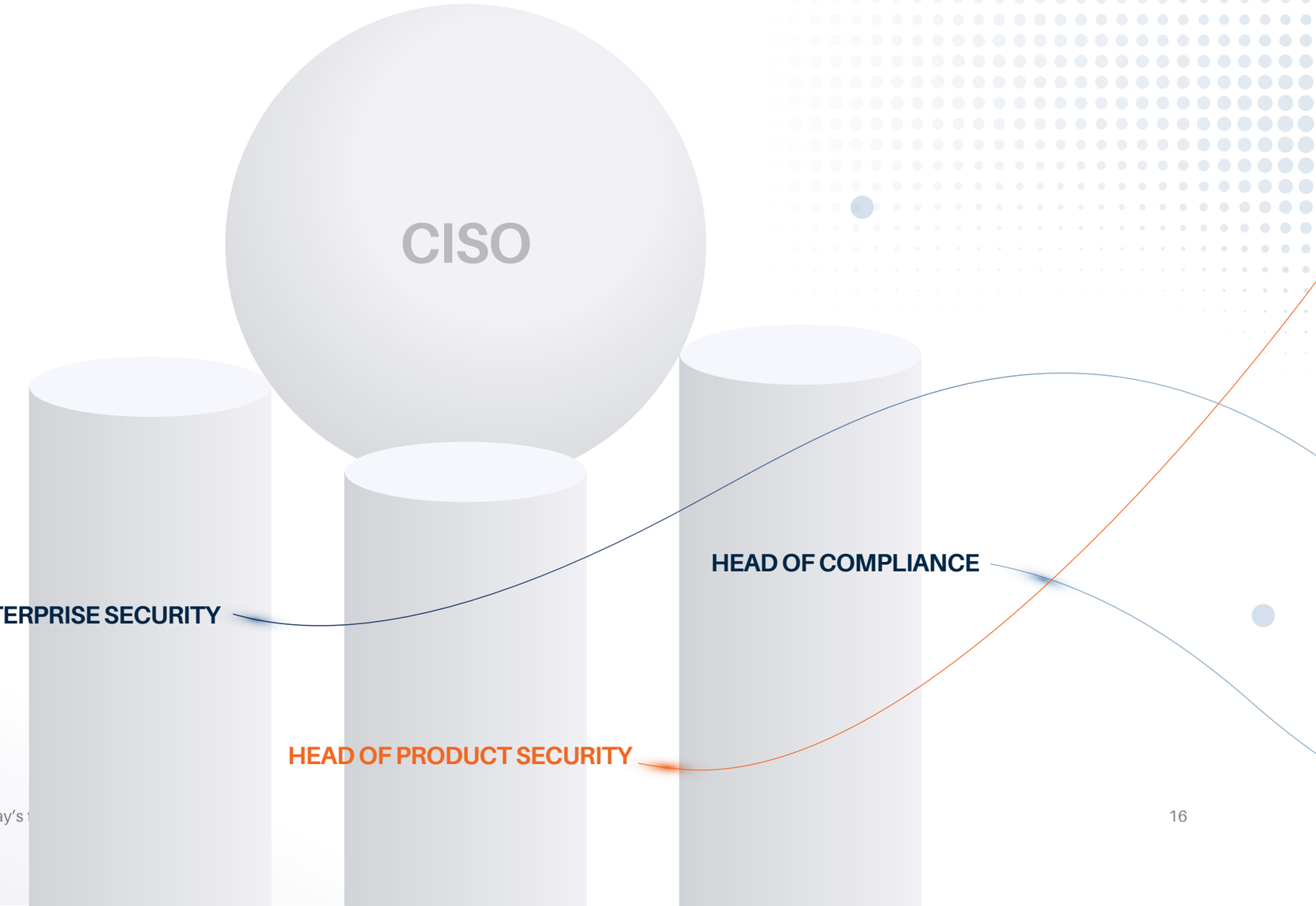
Total cash compensation is comprised of annual salary and on-target bonuses, calculated on an annual basis.

Sign-on and relocation bonuses are not included in total annual cash compensation bonus.

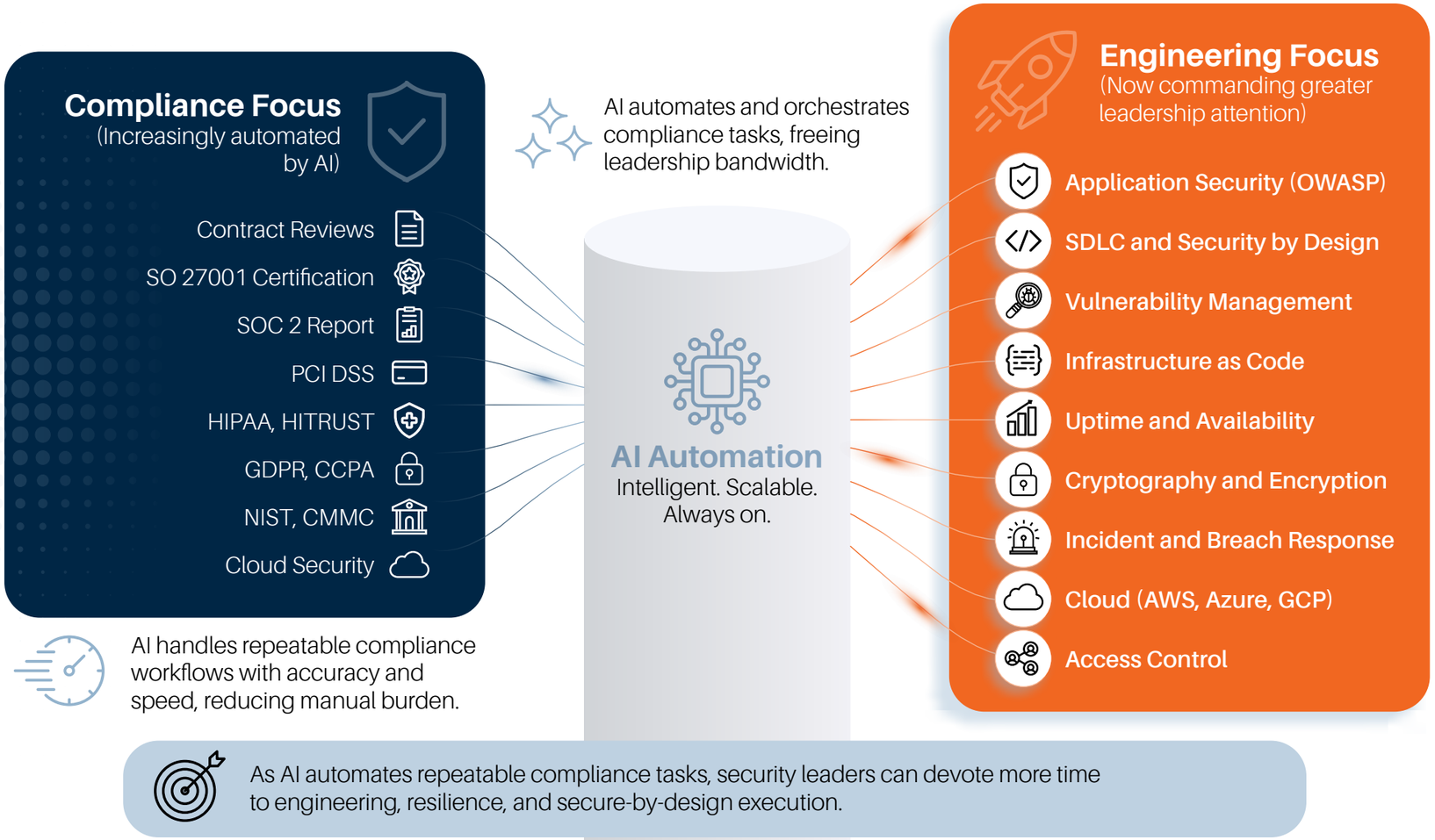
Equity grant is based on companies of all types and classifications and typically reflects estimated gross initial grant (non-annualized).

Structuring a security organization that works

Hiring the right CISO is only step one. Cybersecurity success is defined as much by your organization's security structure as the person overseeing it. Here's how to determine where your CISO should fit in.



AI is shifting cybersecurity leadership from compliance administration to engineering execution



Regardless of your reporting model, if the board and executive team only hear from their CISO during an incident, it's already too late. CISO should meet monthly with the CEO and executive team to outline major risks, investment needs, and emerging regulatory issues, along with quarterly board briefings to discuss directional risk, material developments, and forward-looking priorities.

The CISO's responsibility in the boardroom is to be the translator who can convert technical posture into enterprise risk language to support informed oversight.

In addition, there should be a clear understanding of where authority and decision rights live. In leading organizations, the CISO is responsible for risk assessment and recommendations, while executive leadership and the board retain accountability for material risk acceptance and disclosure. Create clear thresholds that define what can be resolved operationally, what requires CEO alignment, and what warrants board escalation.

Building the bench beyond the CISO

What about execution? Today's high-performing CISOs are focused on building lean internal teams, leveraging AI-enabled tools for scale, and selectively partnering with outside vendors for specialized capabilities such as 24/7 monitoring, pen testing, and surge response.

The minimum viable security team by company stage should include:

Early-stage companies

A hands-on builder CISO plus a small team of security engineers. The internal team focuses on foundational controls, product security integration, and passing enterprise security reviews, while outside partners can provide SOC coverage and compliance support.

Growth-stage companies

A scaling CISO backed by an expanding team across engineering, GRC, and security operations. The internal team focuses on formalizing controls, reducing measurable exposure, and preparing the business for diligence and exit scrutiny, while outside partners can extend capacity for 24/7 monitoring and specialized assessments.

Transformation-stage companies

A commercially-minded CISO supported by a lean team spanning governance, risk, and core detection and response. The internal team focuses on standardizing controls, reducing exposure, and preparing the business for diligence or strategic transition, with external partners extending capacity for 24/7 monitoring and specialized assessments.

Public companies

A governance-oriented CISO supported by dedicated leaders for GRC, security operations, and architecture. The internal team focuses on disclosure discipline, regulatory alignment, and sustained incident readiness across global environments, while outside partners are used selectively for surge response, red teaming, or specific regulatory expertise.

Once the CISO is in place, expect them to hire three lieutenants to help oversee technical execution and governance discipline.

HEAD OF SECURITY ENGINEERING

The Head of Security Engineering is typically a growth-stage hire who is responsible for consolidating architectural integrity, detection and response strategy, and technical control implementation under a single leader. Within the first year, this person should deliver hardened foundational controls, a clarified SOC model, documented architectural risk priorities, and a remediation roadmap aligned to business risk. As the organization scales, this role often separates into dedicated product security, corporate security, and security research roles

HEAD OF GOVERNANCE, RISK, AND COMPLIANCE

The Head of Governance, Risk, and Compliance is responsible for protecting the company's ability to sell, disclose, and operate in regulated markets. Within the first year, this person should help the organization reduce its security questionnaire cycle times, centralize evidence management, create a board-aligned risk policy, and clearly articulate the regulatory roadmap. As compliance processes become increasingly automated, this function often remains a lean, high-impact team of experts rather than scaling headcount.

Setting your cyber leadership hiring process up for success

The CISO hiring market has shifted significantly. Demand is surging, compensation is rising, and top candidates often run multiple processes at once. Organizations that approach hiring with clarity, speed, and a strong value proposition are far more likely to secure top talent. The most effective CISO searches follow a few simple principles.

1. Align the candidate profile to the mandate. Define what the organization truly needs over the next 24-36 months. Is the priority IPO readiness, regulated market expansion, AI-driven product risk, or architectural hardening? The mandate should reflect real business priorities, not a generic security wishlist.

2. Design the role for impact. CISOs want to operate as business executives that are closer to revenue operations, customer expectations, and cross-functional decision-making. That broader mandate is changing reporting expectations as well: burying the CISO several layers down is increasingly incompatible with what top candidates expect and what boards require.

3. Move with structure and speed. Top security leaders have leverage. The market has returned to candidate-driven dynamics, with many CISO candidates running multiple processes at once and frequently ending with several offers. Compensation matters, and so does scope: candidates are looking for authority, access to decision-makers, and the ability to influence the business as much as security operations.

4. Demand technical depth. Across industries, the preference is tilting toward deeply technical security leaders, often with engineering or security research backgrounds. The reason is practical: every company is being reshaped by AI, whether in product or internal productivity, and security leaders are expected to understand what that means and build a plan around it. Forward-thinking CISOs who can translate AI's impact into a credible security roadmap are in especially high demand.

5. Work with a CISO search expert. Cyber leadership hiring is structurally different than traditional executive searches, especially for organizations navigating high-stakes transitions such as pre-IPO, first CISO hires, entering regulated markets, or in the wake of a major incident. An effective partner that specializes in CISO and cyber leader placements can help you refine your mandate, benchmark compensation, identify red flags that may alienate top candidates, and evaluate candidates for strategic and technical fit.

Final takeaway

As boards recalibrate their oversight expectations and AI accelerates the threat cycle, organizations that treat cyber leadership as critical infrastructure instead of overhead have the advantage.

Riviera Partners helps boards and CEOs identify, evaluate, and place the CISOs that are driving this new era of enterprise risk leadership. Our network spans industries, ownership models, and stages of growth, giving organizations access to security leaders who can architect governance, operationalize resilience, and build teams prepared for the realities of 2026 and beyond.

Riviera
PARTNERS

About Riviera Partners

Riviera Partners is a global driver of innovation for today's most influential companies – expertly placing executive talent in the crucial areas of IT, software engineering, product management, security, AI/ML/Data, and design. Riviera combines over two decades of recruiting expertise with a proprietary platform that uses machine learning to score and predict the best candidate for a company's specific needs, driving successful outcomes. As a result, the company has become the go-to talent partner for leading private equity investors, venture capitalists, public companies and technology innovators.

Sean Cleary
Partner & Cybersecurity Practice Lead
Public Companies