CyberRisk Collaborative

Q2 2026

CISO Top 10

Executive Management Priorities

Contents

Priorities Ranked – 2nd Quarter 2026

1	↑	AI/ML/Automation
2	↑	Cloud Security
3	↓	Identity and Access Management (IAM)
4	↓	Data Security
5	↑	Application Security/API Security
6	↓	Supply Chain Cybersecurity
7	↑	Security Operations
8	↓	Vulnerability Management
9	–	Attack Surface Management
10	+	Security Architecture

↑ Rank Up
↓ Rank Down
– Stable
\+ New

CyberRisk Collaborative

Executive Summary

As organizations move deeper into 2026, cybersecurity leadership is transitioning from early-year execution alignment to sustained operational performance and accountability at scale. The Q2 2026 CISO Top 10 - Executive Management Priorities reflects a continued emphasis on governance and measurement, but with a sharper focus on durability, integration, and executive-level influence.

In Q1, CISOs were expected to establish structure, define metrics, and align with business leadership. By Q2, the expectation has evolved, execution is now assumed, and performance is being scrutinized in real time. This shift is evident in the stability at the top of the rankings and the growing importance of leadership, planning, and operational cohesion.

Notably:

- Governance, Risk, and Compliance (GRC) and Security Metrics remain firmly entrenched as the top priorities, reinforcing the central role of measurable, defensible cybersecurity programs.
- Business Continuity and IR / Risk Management continue to decline, not due to reduced importance, but because they are increasingly embedded into operational frameworks rather than treated as standalone priorities.
- Strategic Planning and Leadership Development rise, signaling a shift toward long-term execution sustainability and organizational resilience.
- Technology Selection, Use, and Integration returns to the Top 10, reflecting growing concern around tool sprawl, integration debt, and operational inefficiency.
- Budget and Resource Allocation drops from the rankings, indicating that funding conversations have transitioned into execution discipline and ROI validation.

Call to Action: CISOs must now demonstrate not only execution capability, but repeatable, scalable performance that integrates governance, technology, and leadership into a unified operating model.

Methodology

The CISO Top 10 quarterly report is derived from a comprehensive survey conducted by CyberRisk Collaborative, representing input from 350 CISOs and senior cybersecurity executives. Each respondent identified and ranked their most pressing management concerns for the upcoming quarter, providing both quantitative and qualitative insights. The rankings were then weighted by frequency, assessed for directional change, and analyzed to identify upward or downward trends in strategic emphasis.

This methodology ensures that the report captures not only what CISOs are prioritizing, but also why these priorities are evolving. The analysis reflects both individual executive sentiment and collective industry perspective, providing a real-time pulse of how cybersecurity leadership is responding to shifting regulatory, operational, and financial environments.

About CyberRisk Collaborative

Our mission at the CyberRisk Collaborative (CRC) is to enable career development for current and future cybersecurity leaders. We are a membership community where security practitioners drive curriculum and education, not vendors or analysts. Our goal is to accelerate careers through technology, strategy, and executive management resources, while also saving members time and money with CISO-developed tools, resources, and templates. By joining CRC, our members expand their networks with exclusive access to a global community of top cybersecurity leaders and stay ahead of threats with cutting-edge tools and insights to protect their organizations.

Key Trends Shaping Q2 2026

1. Governance and Metrics Have Become the Operating Backbone

GRC and Security Metrics holding the top two positions, both trending upward, confirms a structural shift first established in Q1. However, in Q2, these are no longer emerging priorities, they are now baseline expectations.

- GRC is evolving into continuous, real-time governance, tightly integrated with enterprise risk decisions.
- Security Metrics are being judged on business relevance, not technical completeness.

Implication: CISOs are being evaluated on their ability to operationalize governance through measurable outcomes, not just frameworks or reporting.

2. Risk and Resilience Are Becoming Invisible Infrastructure

Business Continuity and IR / Risk Management both decline again in Q2. This is not a deprioritization, it is a signal of maturity.

In Q1, continuity and response were transitioning from reactive focus areas into structured programs. In Q2, they are increasingly:

- Embedded into governance models
- Integrated into enterprise planning
- Expected to function without executive escalation

Implication: CISOs are no longer rewarded for response capability alone, but for predictability, automation, and integration of risk management into daily operations.

Key Trends Shaping Q2 2026

3. Strategic Planning Is Now a Core Execution Discipline

Strategic Planning rises again in Q2, reflecting a critical shift:

- Planning is no longer periodic, it is continuous and adaptive
- Roadmaps are expected to demonstrate progress, not intent
- Strategy must now directly tie to metrics, funding, and outcomes

This builds directly on Q1's transition from budget approval to execution oversight, but Q2 introduces a higher bar, strategy must prove it is working.

Implication: CISOs must operate with product-management rigor, continuously refining priorities based on performance data.

4. Leadership and Organizational Resilience Are Rising

Leadership Development moves up in Q2, reversing its stagnation in Q1 where it remained a recognized but underfunded risk.

This shift reflects mounting pressure from:

- Burnout and retention challenges
- Succession planning gaps
- Increasing complexity of the CISO role

Implication: Organizations are beginning to recognize that execution at scale requires leadership depth, not just technical capability.

Key Trends Shaping Q2 2026

5. Stakeholder Engagement Is Under Pressure

Stakeholder / Board Engagement declines in Q2 after re-entering in Q1. This suggests:

- Initial executive alignment has been established
- Ongoing engagement is becoming harder to sustain
- Boards are shifting from listening to evaluating

Implication: CISOs must move from narrative-building to performance demonstration, maintaining credibility through outcomes rather than communication alone.

6. Technology Integration Emerges as a Leadership Priority

The return of Technology Selection, Use, and Integration at #10 is one of the most important signals in Q2.

This aligns directly with the broader trend seen in the Q1 Technology report, where CISOs were already shifting from expansion to optimization and efficiency.

Key drivers:

- Tool sprawl and overlapping capabilities
- Integration complexity across security stacks
- Pressure to extract value from existing investments

Implication: Technology strategy is no longer about acquisition, it is about integration, rationalization, and operational coherence.

Priority Analysis (Q2 2026)

↑ Rank Up ↓ Rank Down — Stable + Returning

RANK PRIORITY

01 ↑ **Governance, Risk, and Compliance (GRC)**
Remains the top priority as organizations demand continuous, defensible governance models integrated into enterprise decision-making.

Call to Action: Operationalize GRC through real-time dashboards, ownership clarity, and board-level transparency.

02 ↑ **Security Metrics**
Continues to rise as CISOs are measured on business-aligned performance indicators, not technical outputs.

Call to Action: Align metrics with financial and operational outcomes; eliminate vanity metrics.

03 ↓ **Business Continuity**
Declines further as resilience becomes institutionalized within governance and planning frameworks.

Call to Action: Embed continuity into enterprise architecture and decision-making processes.

04 ↓ **IR / Risk Management**
Shifts from reactive capability to structured, predictable execution models.

Call to Action: Formalize escalation, authority, and financial impact modeling.

05 ↑ **Strategic Planning**
Rises as execution accountability increases.

Call to Action: Continuously refine roadmaps with measurable milestones and adaptive prioritization.

RANK PRIORITY

06 ↓ **Data Privacy**
Declines as baseline programs stabilize, though AI-driven complexity continues to build beneath the surface.

Call to Action: Integrate privacy into broader data and AI governance frameworks.

07 ↑ **Leadership Development**
Moves up as organizations confront burnout, succession risk, and scaling challenges.

Call to Action: Institutionalize leadership pipelines and mentoring frameworks.

08 ↓ **Stakeholder / Board Engagement**
Drops as executive relationships shift from alignment to performance evaluation.

Call to Action: Maintain credibility through measurable outcomes and forward-looking risk narratives.

09 — **Role of the CISO**
Remains stable, reflecting that the role is now well-defined and expected to deliver consistently.

Call to Action: Focus on execution excellence and cross-functional leadership impact.

10 + **Technology Selection, Use, and Integration**
Re-enters as organizations confront integration debt and inefficiency across security stacks.

Call to Action: Rationalize tools, prioritize interoperability, and align technology to measurable outcomes.

What Dropped

Budget and Resource Allocation

Budget and Resource Allocation falls out of the Top 10 in Q2 after remaining stable in Q1.

This reflects a clear transition:

- Funding is no longer the primary concern
- Execution and ROI are now under scrutiny

Implication: CISOs must demonstrate financial discipline through outcomes, not budget acquisition.

Closing Perspective

The Q2 2026 Executive Management priorities confirm a defining shift in the CISO role:

- From strategy to execution
- From execution to measurable performance
- From performance to sustained, scalable operations

Cybersecurity leadership is now judged on its ability to function as a predictable, integrated business capability, not a reactive technical function..

Final Call to Action: CISOs must evolve into operational executives, capable of aligning governance, technology, and leadership into a unified system that delivers continuous, measurable business value.

About

About CyberRisk Alliance

CyberRisk Alliance provides business intelligence that helps the cybersecurity ecosystem connect, share knowledge, accelerate careers, and make smarter and faster decisions. Through our trusted information brands, network of experts, and innovative events we provide cybersecurity professionals with actionable insights and act as a powerful extension of cybersecurity marketing teams. Our brands include SC Media, the Official Cybersecurity Summits, Security Weekly, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, Cybersecurity Collaborative, ChannelE2E, MSSP Alert, LaunchTech Communications, Execweb and Channel Pro Networks.

Learn more at www.cyberriskalliance.com.

