CyberRisk Collaborative

Q1 2026

CISO Top 10

Executive Management Priorities

CISO Top 10
Executive Management

As organizations transition from the close of the 2025 calendar year into Q1 2026, cybersecurity leadership priorities reflect a decisive shift from retrospective accountability to forward execution. Year-end audits, regulatory disclosures, incident reviews, and budget approvals have elevated expectations for structure, discipline, and predictability across security programs. The Q1 2026 CISO Top 10 – Executive Management Priorities illustrates how CISOs are translating lessons learned in 2025 into governance maturity, measurable performance, and executive alignment. Governance, metrics, and strategic execution now dominate, signaling that CISOs are no longer being evaluated on intent or activity, but on sustained delivery and business relevance.

Call to Action: CISOs must enter 2026 prepared to operate as execution-focused executives, converting strategy into operating rhythm early in the year.

CyberRisk Collaborative

Contents

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. Together, these inputs form a reliable and data-backed representation of the evolving executive management landscape.

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.

RANK PRIORITY CHANGE

↑ 01 Governance, Risk, and Compliance (GRC)

↑ Up from #2

Governance, Risk, and Compliance rises to the top position in Q1 2026, reflecting its role as the primary mechanism through which cybersecurity earns executive and board trust. Following year-end disclosures and audit cycles, organizations are under pressure to prove that risk oversight is continuous, defensible, and integrated into enterprise decision-making. CISOs are increasingly expected to unify regulatory obligations, enterprise risk tolerance, and security controls into a coherent operating model that supports real-time governance. The elevation of GRC also reflects intensifying regulatory enforcement and board scrutiny. In Q1, GRC is no longer viewed as compliance hygiene—it is the structural foundation for cybersecurity leadership credibility.

Call to Action: Shift GRC from periodic reporting to continuous governance with real-time risk dashboards and clear ownership models.

↑ 02 Security Metrics

↑ Rank Up

Security Metrics continues its upward trajectory as CISOs face heightened expectations to demonstrate measurable value from cybersecurity investments. With budgets approved at year-end, Q1 shifts attention from funding justification to execution accountability, requiring leaders to prove that spend translates into risk reduction and operational resilience. Boards increasingly favor business-outcome metrics over technical activity measures. This evolution reflects a maturation of the CISO role into one requiring fluency in performance management and financial language.

Call to Action: Rationalize metrics and align them with CFO and COO priorities, focusing on outcome-driven indicators.

CyberRisk Collaborative

RANK PRIORITY CHANGE

↓ 03 Business Continuity

↓ Down from **#1**

Business Continuity declines from its year-end dominance as organizations move from crisis reflection to operational normalization. Q4 incident reviews elevated continuity concerns, but in Q1 these expectations are embedded into governance and planning cycles. This reflects maturity rather than reduced importance, as continuity becomes institutionalized. CISOs are expected to integrate resilience across business units and technology decisions.

Call to Action: Embed continuity requirements into enterprise governance and strategic planning.

↓ 04 IR / Risk Management

↓ Rank Down

Incident Response and Risk Management remains critical, though expectations for discipline and predictability are rising. Executives are less tolerant of ad hoc response models following year-end reviews. CISOs must demonstrate defined escalation paths, authority, and financial impact modeling. The emphasis has shifted from heroics to controlled execution.

Call to Action: Formalize IR authority models and decision thresholds before incidents occur.

↓ 05 Data Privacy

↓ Rank Down

Data Privacy slips modestly as baseline compliance programs stabilize entering 2026. However, AI-driven data use introduces new governance complexity. CISOs must balance privacy oversight with broader execution priorities. Privacy risk may resurface later as AI regulation accelerates.

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

CyberRisk Collaborative

RANK	PRIORITY	CHANGE
↑ 06	Strategic Planning	↑ Rank Up

Strategic Planning rises as organizations move from budget approval to execution oversight. CISOs are under pressure to translate strategy into operational outcomes through adaptive roadmaps. Planning is now continuous rather than annual, serving as the bridge between governance intent and delivery accountability.

Call to Action: Define clear milestones and success criteria to sustain executive confidence.

RANK	PRIORITY	CHANGE
+ 07	Stakeholder / Board Engagement	+ Returning

Stakeholder and Board Engagement returns as CISOs reset executive relationships after year-end reporting. Boards seek clarity on forward-looking risk posture and investment effectiveness. Early-year engagement often determines influence for the remainder of the year.

Call to Action: Proactively engage boards early with forward-looking narratives and priorities.

RANK PRIORITY CHANGE

08 Role of the CISO

Rank Down

The Role of the CISO declines slightly because its strategic relevance is now assumed. Attention has shifted from defining the role to evaluating performance within it. CISOs are judged on execution quality and cross-functional leadership.

Call to Action: Focus on delivery excellence rather than role positioning.

09 Leadership Development

No Change

Leadership Development remains a persistent weakness despite recognition of its importance. Burnout and succession risk continue as investment is deferred in favor of execution demands. This creates long-term fragility even as short-term performance improves.

Call to Action: Institutionalize leadership development through mentoring and succession planning.

10 Budget and Resource Allocation

Trending Up

Ranking Unchanged

Budget and Resource Allocation remains stable as organizations enter execution mode. Focus shifts from securing funding to demonstrating disciplined spend and measurable return. Budget credibility is earned through execution.

Call to Action: Tie spending directly to outcomes and revisit assumptions regularly.

CyberRisk Collaborative

About

CyberRisk ALLIANCE

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.

CyberRisk Collaborative