CyberRisk Collaborative

Q2 2026

CISO Top 10
Technology 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
- ↗ Trending Up *Rank Unchanged*
- ↓ Rank Down
- ↘ Trending Down *Rank Unchanged*
- \+ New

CyberRisk Collaborative

Executive Summary

As organizations advance through 2026, cybersecurity technology strategy is undergoing a decisive shift from optimization to orchestration. The Q2 2026 CISO Top 10 - Technology Priorities reflects an environment where foundational technologies remain critical, but success is increasingly defined by how effectively they are integrated, automated, and aligned to business outcomes.

In Q1, CISOs focused on extracting value from existing platforms and reducing complexity. By Q2, that mandate has intensified, technology performance is now measured by interoperability, scalability, and measurable risk reduction.

Key developments include:

- AI / ML / Automation rises to the #1 position, signaling a transition from experimentation to operational dependency.
- Cloud Security drops from #1 to #2, reflecting maturity in adoption and a shift toward governance and cost control.
- Identity and Access Management (IAM) moves up, reinforcing its role as the control plane for modern security architectures.
- Security Operations and Supply Chain Cybersecurity trend upward, highlighting increased focus on execution efficiency and external risk exposure.
- Security Architecture enters the Top 10 as a new priority, underscoring the growing need for cohesive, integrated security design.
- Zero Trust drops out of the rankings, indicating that its principles are being absorbed into broader identity, architecture, and access strategies.

Call to Action: CISOs must move beyond optimizing individual tools and instead build integrated, intelligent security ecosystems that deliver consistent, scalable outcomes.

Methodology

The CISO Top 10 rankings were derived from structured interviews and one-on-one surveys with 350 CISOs and equivalent senior cybersecurity executives, representing sectors including healthcare, finance, manufacturing, and government. Participants were asked to identify their most pressing technology priorities, rank them by importance, and provide qualitative insights explaining their rationale. Responses were analyzed both for frequency and trend direction, enabling the identification of rising, stable, or declining priorities.

By triangulating quantitative ranking data with qualitative community commentary, this methodology captures not only the 'what' but also the 'why' behind each ranking shift. It also reflects the broader sentiment of security leaders navigating rapid technological convergence, increased automation, and growing board-level accountability. The result is a reliable, comparative view of where CISOs are investing time, resources, and executive attention.

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. AI Becomes the Operational Core of Cybersecurity

AI / ML / Automation rising to #1 marks a critical inflection point. In Q1, AI was positioned as an enabler of scale with increasing governance requirements. In Q2, it has become:

- A core operational dependency across detection, response, and analysis
- A driver of efficiency in understaffed security organizations
- A mechanism for reducing human-driven bottlenecks

However, this rise also introduces new pressures:

- Explainability and auditability
- Risk of over-automation
- Integration with existing workflows

Implication: AI is no longer a capability layer, it is becoming the execution engine of modern security operations.

2. Cloud Security Stabilizes as a Governance Challenge

Cloud Security's drop to #2 does not indicate reduced importance, it reflects increasing maturity.

In Q1, the focus had already shifted from adoption to governance, configuration discipline, and cost control. In Q2:

- Core cloud security controls are broadly established
- The challenge is now consistency, visibility, and cost efficiency at scale

Implication: Cloud security is transitioning from a priority initiative to an operational baseline, where execution quality defines effectiveness.

Key Trends Shaping Q2 2026

3. Identity Becomes the Central Control Plane

Identity and Access Management rising to #3 reinforces a structural reality:

- Identity is now the primary enforcement layer across cloud, applications, and endpoints
- Zero Trust principles are increasingly implemented through IAM capabilities

With Zero Trust dropping from the rankings, its concepts are being absorbed into:

- Identity governance
- Access controls
- Adaptive authentication models

Implication: Identity is no longer foundational, it is central to enforcing all modern security architectures.

4. Data Security and Privacy Complexity Continues to Slow Progress

Data Security declines again in Q2, reflecting persistent execution challenges first seen in Q1.

Key issues include:

- Data discovery and classification complexity
- Fragmentation across platforms
- Intersection with AI and privacy requirements

Implication: Despite its importance, Data Security remains constrained by implementation difficulty and cross-domain dependencies.

Key Trends Shaping Q2 2026

5. Application and API Security Reflects Stable but Growing Risk

Application Security / API Security trends upward, driven by:

- Continued growth in API ecosystems
- Increased development velocity
- Expanding attack surfaces

The emphasis remains on:

- Automation within DevSecOps pipelines
- Early integration into development workflows

Implication: Application security is evolving into a continuous, automated discipline, rather than a testing phase.

6. Operational Efficiency Becomes a Competitive Advantage

Security Operations and Vulnerability Management both trend upward, highlighting a renewed focus on execution efficiency.

- Vulnerability Management continues its shift toward risk-based prioritization
- Security Operations is focused on automation, orchestration, and fatigue reduction

These trends reflect a broader reality:

- Security teams must do more with constrained resources
- Performance is measured by speed, consistency, and impact

Implication: Operational excellence is now a primary differentiator for security programs .

Key Trends Shaping Q2 2026

7. External Risk and Exposure Management Gain Importance

Supply Chain Cybersecurity and Attack Surface Management both trend upward in Q2.

This reflects:

- Increased awareness of third-party and dependency risk
- A shift from discovery to remediation and impact prioritization

Implication: CISOs are expanding focus beyond internal controls to ecosystem-wide risk management.

8. Security Architecture Emerges as a Strategic Priority

Security Architecture enters the Top 10 as a new priority, signaling a critical shift:

- Organizations are struggling with fragmented security stacks
- Integration challenges are limiting the effectiveness of existing tools
- There is a growing need for cohesive, scalable design principles

This directly aligns with the broader Q2 Executive Management trend around technology integration.

Implication: Security architecture is becoming the foundation for long-term scalability and efficiency, not just a design function.

Priority Analysis (Q2 2026)

Rank Up | Trending Up | Rank Down | Trending Down | New

RANK PRIORITY

01 AI/ML/Automation

Rises to the top as AI becomes central to scaling detection, response, and analysis.

Call to Action: Deploy AI with governance guardrails and integrate it into core workflows with measurable outcomes.

02 Cloud Security

Drops slightly as organizations shift focus from adoption to governance and operational discipline.

Call to Action: Enforce consistent controls and optimize cost, configuration, and visibility.

03 Identity and Access Management (IAM)

Moves up as identity becomes the primary enforcement layer across environments.

Call to Action: Strengthen identity governance and continuous access validation.

04 Data Security

Declines due to ongoing execution complexity.

Call to Action: Invest in integrated discovery, classification, and governance capabilities.

05 Application Security/API Security

Remains critical as attack surfaces expand.

Call to Action: Embed automated security into development and runtime environments.

RANK PRIORITY

06 Supply Chain Cybersecurity

Rises as third-party risk becomes more visible and persistent.

Call to Action: Implement continuous monitoring and shared accountability models.

07 Security Operations

Moves up as organizations prioritize efficiency, automation, and consistency.

Call to Action: Standardize processes and deploy AI-driven orchestration.

08 Vulnerability Management

Declines slightly despite continued importance.

Call to Action: Prioritize vulnerabilities based on exploitability and business impact.

09 Attack Surface Management

Maintains momentum as focus shifts to remediation and exposure reduction.

Call to Action: Integrate exposure data into remediation workflows.

10 Security Architecture

Enters the Top 10 as organizations confront integration challenges and architectural fragmentation.

Call to Action: Establish unified architecture frameworks that prioritize interoperability and scalability.

What Dropped

Zero Trust

Zero Trust falls out of the Top 10 in Q2 despite trending upward in Q1.

This reflects a maturation rather than a decline:

- Zero Trust principles are now embedded within IAM, cloud, and architecture strategies
- It is no longer treated as a standalone initiative

Implication: Zero Trust has transitioned from a strategic concept to an operational reality.

Closing Perspective

The Q2 2026 Technology priorities highlight a critical evolution:

- From tool adoption to optimization
- From optimization to integration
- From integration to intelligent orchestration

Cybersecurity technology is no longer judged by its capabilities alone, but by its ability to operate as a cohesive, automated, and measurable system.

Final Call to Action: CISOs must architect security ecosystems that are integrated by design, automated by default, and measurable in impact, ensuring that technology investments translate into sustained risk reduction and operational resilience.

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.

