ARTIFICIAL INTELLIGENCE

How CEOs Should Manage Escalating Cybersecurity Risks in the Age of AI

By Vanessa Lyon, Vladimir Lukic, and Alex Asen

ARTICLE AUGUST 14, 2026 8 MIN READ

BCG research shows that CEOs have taken the lead on AI strategy. AI investments have nearly doubled since last year, and 82% of CEOs believe that AI innovations will yield a positive ROI in 2026.

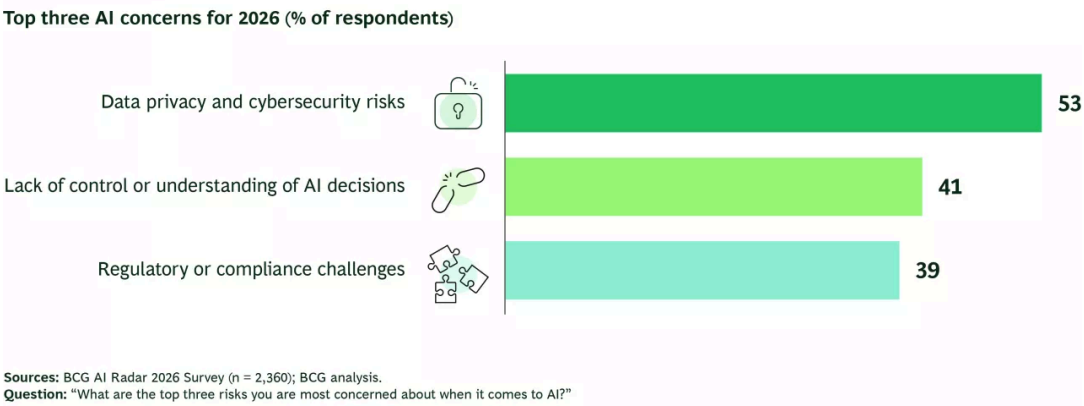
©2026 Boston Consulting Group

Enthusiasm for AI is high, but half of CEOs surveyed acknowledge that if they get AI wrong, their jobs are on the line. Of course, there are innumerable ways to fail with the technology, but CEOs understand that AI-enabled cybersecurity threats are existential.

The State of Cybersecurity Risk Today

Although CEOs rank cyber threats as a top-three risk to their business, companies have so far largely failed to modernize their cybersecurity strategy. (See the exhibit.)

Leaders Say Data Privacy and Cybersecurity Are the Top AI Concerns



Inertia, along with an inability to know exactly how to adapt cybersecurity to the AI era, has taken hold across many enterprises. Beyond that, a robust investment in AI aligns with a CEO's natural excitement about possibilities for growth and innovation. Cybersecurity—despite being an AI initiative in and of itself—is unglamorous by comparison.

The best a CEO can hope for is that nothing bad will happen. And in that case, it is difficult to prove the investment in risk mitigation is worthwhile.

But in a world where frontier models are capable of exploiting vulnerabilities across major operating systems, the imperative to act with urgency is clear. Cybersecurity can no longer be siloed as an issue for the chief information security officer (CISO) or chief information officer (CIO) to handle independently of organization leadership, or as a strictly technical issue.

Cybersecurity strategy in the age of AI requires top-down and bottom-up enterprise-wide coordination. Just as CEOs have taken the lead on AI innovation, they must embrace their

©2026 Boston Consulting Group

position at the top of a pyramid where precise communication and clear delegation of decision rights can mean the difference between a secure organization and an insecure one.

CEO Actions to Drive Cybersecurity Resilience in the AI Era

CEOs can take a number of actions to drive alignment and clarify roles and responsibilities in key moments to avoid imperiling the organization. CEOs need not be security experts, but they should understand how broad the surface area of cyber risk is in an environment where both organizations and cyber attackers benefit from generative AI. AI-enabled cyber threats grow stronger all the time, and an organization's vulnerabilities increase as its own AI use grows.

It is essential that CEOs be proactive, avoid complacency, and reject any impulse to let inertia win out, regardless of how ill-defined the breadth of the problem may be. BCG's 2026 CISO Survey found that 35% of organizations report having experienced significant impact from AI-enabled attacks in the preceding twelve months. They cite data leakage as the greatest AI risk, with the average organization reporting three significant breaches and 25 sensitive data incidents.

In light of baseline acceptance that attacks are inevitable and breaches are likely, strategies for containment of major attacks and for ongoing resilience are of paramount importance. To create a cybersecurity operating model appropriate for the AI era, CEOs must drive five key actions:

- Prioritize the organization's crown jewels.
- Plan for prevention to fail.
- Govern AI ecosystem risk.
- Secure AI by design.

©2026 Boston Consulting Group

- Empower a cross-functional team to react quickly.

An organization's ability to withstand persistent AI-enabled threats will likely depend on its having a CEO who takes these actions while embracing an always-on strategy that starts with foundational cybersecurity hygiene.

Prioritize the Organization's Crown Jewels

An organization's crown jewels are the critical assets and key processes that would lead to existential harm if compromised. These include, among others, intellectual property, sensitive data, credentials and access, and operational systems.

Because security resources—including budget, talent, and leadership attention—are finite, CEOs must prioritize protection of their crown jewels, ensuring that they concentrate scarce resources on what matters most, rather than spreading them evenly across assets of unequal importance.

To ensure their security, CEOs must know what the crown jewels are and must take ownership of them. In practical terms, CEOs should mandate that their business, IT, and security teams liaise to create a map that includes the crown jewels themselves and an explanation of why each asset is vital to the organization. The map should specify the business context of each crucial asset, including the key stakeholder owner, department, business dependencies, and impact to the business if compromised. The CEO should own a board-approved risk statement detailing this information, together with an explanation of the broad ramifications of failure if a cyber attack compromises the organization.

Plan for Prevention to Fail

©2026 Boston Consulting Group

As cyber attacks become inevitable, an organization's long-term security will likely depend on its ability to detect and respond to incidents swiftly. CEOs should ensure that the security team establishes clear, measurable goals to minimize reaction time and protect key operations.

Two key metrics that security teams should establish thresholds for are mean time to detect and mean time to recover. Historically, these metrics measured average performance in days or even months; but in today's AI-powered world, leading companies are setting thresholds that measure in minutes. Identifying and committing to such concrete benchmarks will help organizations drive clarity about what is possible and what is necessary to protect the organization.

CEOs should also oversee the creation of immutable backups or carefully guarded and maintained offline storage of encrypted backups of key systems and databases.

In addition, CEOs should approve an executive crisis playbook that specifies key decision-making stakeholders and operations. To test this playbook, CEOs should invest in and participate in multiple cybersecurity crisis simulations each year. These measures will help communicate the importance of an organization-wide approach to cybersecurity while also concretely establishing accountability.

Govern AI Ecosystem Risk

Just as CEOs partner with their boards to determine how much concentration risk their company can tolerate from a financial perspective, they must gain clarity from cybersecurity and risk leaders about ecosystem risks.

AI multiplies dependencies on third parties, including hyperscalers, model providers, software-as-a-service copilots, embedded AI features, and tool/plug-in ecosystems. CEOs must ensure that their organization resists over-indexing on a single vendor partner or model solution.

CEOs must ensure that their risk and security executives do the following:

- **Tier vendors, and align controls accordingly.** This task involves identifying which third parties are most critical to the business and applying rigorous security, oversight, and resilience requirements on the basis of the level of risk they pose.
- **Establish exit plans for systemic dependencies.** Security teams should develop and regularly validate contingency plans for quickly replacing or operating without a critical vendor if it experiences a cyber attack, outage, or business failure.
- **Create stress tests to assess vendor-failure scenarios.** Regularly simulating the sudden loss or compromise of key vendors will help the organization identify operational weaknesses,

©2026 Boston Consulting Group

validate response plans, and improve organizational resilience

Secure AI by Design

As organizations increasingly weave AI systems into the fabric of their processes and operations, CEOs must shift their thinking about cybersecurity, fully incorporating it into the ideation and building phase of new products and processes. It is not something to address after the fact.

CEOs should embrace a secure-by-design mentality that empowers security experts and product builders to treat security as a key enabler on the roadmap to new products and to embed it into AI product teams to ensure that the organization builds products properly from the outset.

To make secure-by-design scalable rather than a bottleneck, security and engineering leaders should develop a library of reusable security building blocks—preapproved architecture patterns, code templates, and configuration standards that teams can adopt by default. When secure components are readily available and simple to implement, teams don't need to solve security problems from scratch on every project, accelerating delivery and reducing the risk of inconsistent or ad hoc security decisions across the organization.

The organization can then publicize the required tooling, permissions, and approvals, creating a transparent culture for building securely by design. The secure-by-design methodology aims to reduce red tape by enabling teams to avoid getting tangled up in lengthy approvals processes. Instead, they will know what is required and will account for it from the origination phase.

Empower a Cross-Functional Team to React Quickly

Security is a team endeavor. Specifically, CEOs can advance a united approach in three ways:

- **Get the board on board.** A CEO should aim to create airtight cohesion with the organization's board. Doing this involves liaising with the chief risk officer (CRO) to articulate the breadth of the risks that the organization faces. Then, the CEO and the board can agree on a philosophy of resourcing versus risk tolerance.

©2026 Boston Consulting Group

- **Align security in the C-suite.** Once the CEO and the board are fully in tune, the CEO should establish clear coordination and decision rights among the C-suite's three key security leaders—the CISO, the CRO, and the CIO/CTO.
- **Initiate cross-functional coordination.** The CEO should initiate an organization-wide effort to transform cybersecurity for the AI era.

Multiple teams play key roles in cross-functional coordination, although the optimal structure will vary by organization and industry:

- **The CISO and the security team** set standards and coordinate responses across the organization.
- **The CRO** owns risk policy, risk appetite, and risk monitoring across business units.
- **The CTO and IT operations** deliver continuous monitoring, hardening, and business continuity planning.
- **The heads of product development and engineering** own coding security and embed scanning into continuous integration and continuous delivery.
- **The chief legal officer and legal and insurance** teams manage coverage, regulatory exposure, and disclosure requirements.
- **The head of procurement** manages third-party and supply chain risk.
- **Human resources** builds a security-aware culture through onboarding, training, and performance expectations.
- **Communications** manages internal and external messaging, preserving trust with customers, employees, and the market.
- **Business unit heads** are responsible for risk ownership and control implementation within their own functions.
- **Internal audit** independently tests security controls, providing another layer of assurance.

Only the CEO can deliver the mandate to align key leaders in a way that communicates the critical importance of cross-functional ownership of security.

Ultimately, a CEO's role as an organization's cybersecurity leader is to communicate in no uncertain terms that security is everyone's problem and opportunity. Risk will always exist, and

©2026 Boston Consulting Group

the level of threat will continue to expand, so organizations must shift to an always-on approach to resilience—and the time to act is yesterday.

About BCG's Center for Leadership in Cyber Security

As digital transformation accelerates, it opens new frontiers for innovation, growth, and competitive advantage—but also heightened vulnerabilities. Cyber is no longer just a technical concern; it's a strategic imperative. Organizations must evolve their cyber posture in tandem with digital progress to safeguard trust and enable resilience.

BCG's Center for Leadership in Cyber Strategy applies bold, business-first thinking to reframe cybersecurity as integral to business strategy—not an afterthought. We embed "security by design" into how leaders shape, evaluate, and execute priorities from the outset. Drawing on BCG's global network of cybersecurity, risk, and strategy experts, we help executives cut through technical complexity and fear-driven narratives. By reframing digital risk in business and economic terms, we empower confident decision-making that turns resilience into a source of lasting competitive edge—enabling organizations to innovate, adapt, and emerge stronger through disruption. More information on BCG's Center for Leadership in Cyber Strategy can be found here.

©2026 Boston Consulting Group

Authors

Vanessa Lyon

Managing Director & Senior Partner
New York

Vladimir Lukic

Managing Director & Senior Partner; Global Leader, Tech and Digital Advantage
Boston

Alex Asen

Senior Director
ACC – Boston

ABOUT BOSTON CONSULTING GROUP

Boston Consulting Group bridges the gap between ambition and outcomes for the world's leading companies and organizations. We are built for this era of unprecedented change — bringing strategic clarity rooted in over 60 years of deep domain knowledge, combined with applied AI shaped by our practitioners. BCG works shoulder-to-shoulder with CEOs across industries and geographies to deliver transformative impact at scale: stronger returns, transferred capabilities, and change that sticks. For more information, visit bcg.com.

©2026 Boston Consulting Group