Gartner Business Quarterly

Fourth Quarter 2026

Derisk AI to create value at scale

→ Close the AI Risk Gap to Generate Value at Scale

→ Contain AI-Related Cybersecurity Risk Without Slowing the Business

Gartner®

Contents

The AI Value Gap Is Really an AI Risk Gap

"To create and safeguard AI value at scale, you must plan to spend at least twice as much on derisking AI as you spend on the tools themselves."

While generative AI pilots often demonstrate exciting upfront value, they also create a dangerous illusion of safety. Severe operational, financial, and security vulnerabilities inevitably explode when you scale GenAI tools into production, threatening to stall your initiatives or saddle your enterprise with an untrustworthy system.

Only 23% of CxOs are confident in their organization's generative AI outputs.

To cross the chasm from being "ready to fail" to "ready to scale," executive leaders must proactively close the AI risk gap across three critical pillars: **cost**, **cybersecurity**, and **trustworthiness**. Miss even one of these pillars, and you will fail to protect the enterprise value you intend to create.

Closing this risk gap requires serious investment that most organizations underestimate. To create and safeguard AI value at scale, you must plan to spend at least twice as much on derisking AI as you spend on the tools themselves. Without this commitment, you risk failure.

This issue of the *Gartner Business Quarterly* will help you protect AI value. We explain how to manage the specific drivers that make AI costs materially more unpredictable than those in previous technology disruptions, and how to contain AI-related cybersecurity risk without slowing the business. We show you how to build real-time AI governance, develop enterprise context that gives AI the right information at the right time, and make human "guardians" your last line of defense. We also warn that an operational "readiness gap" may hamper CEOs' AI ambitions and argue that enterprises should view AI as a sociological phenomenon rather than just a set of technologies.

— Rita Sallam and Mary Mesaglio
Distinguished VP Analysts and Chiefs of Research

4Q

CEO Watch

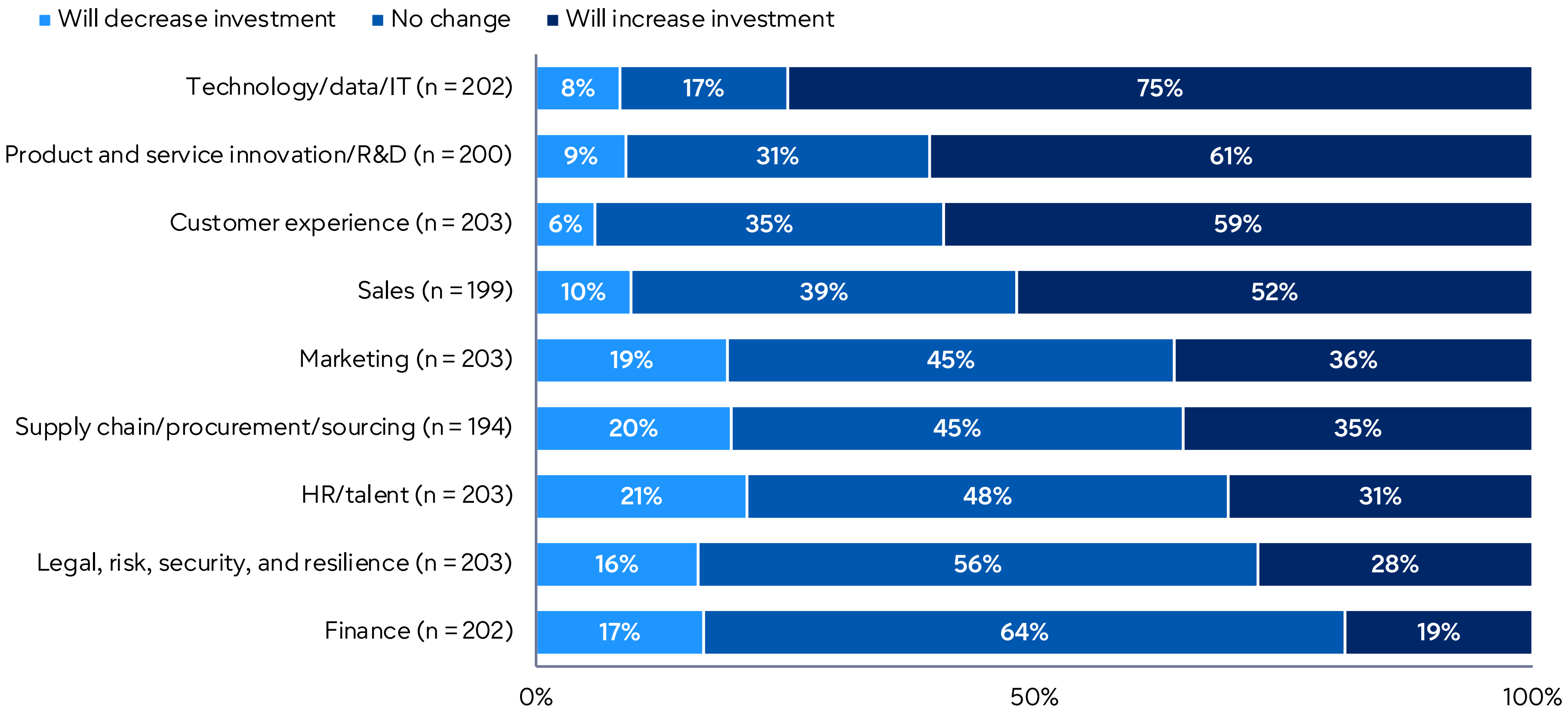
AI Investments Reveal a Dangerous Readiness Gap

by David Furlonger

26

Organizations know AI will transform competitive dynamics, operating models, and decision-making structures. But data from the 2027 Gartner CEO Survey highlight a shortage of operational preparedness as the most important AI challenge facing CEOs.

Figure 1: CEO Investment Change Intentions for 2027



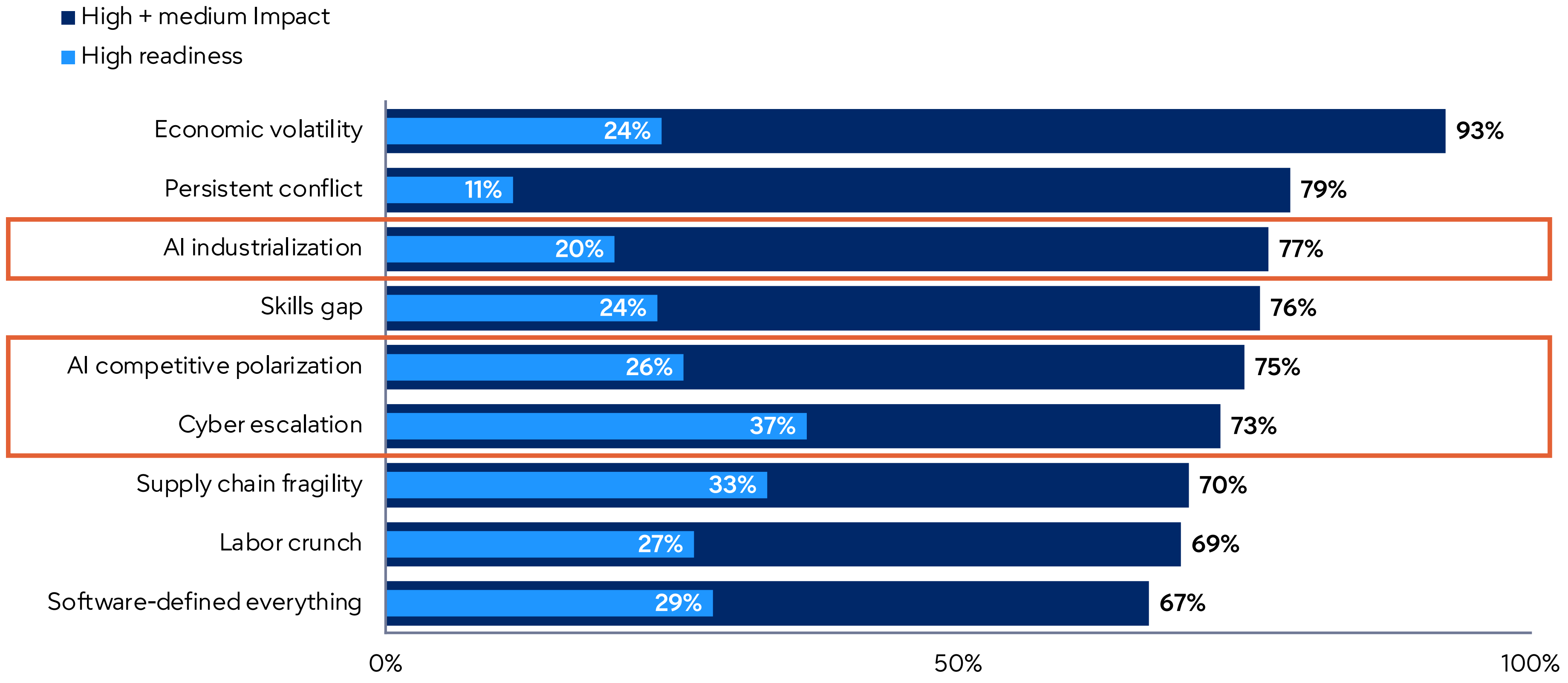
n = varies CEOs and Senior Business Executives; excluding not applicable
Q. Compared to the last fiscal year, how will your organization's financial investment in the following functions/areas change through 2027?
Source: 2027 Gartner CEO Survey. Conducted April -May 2026 among 203 global CEOs and senior business executives. Fielded by Gartner using an external panel.

This gap shows up in two main ways:

A structural imbalance in investment priorities. Although 75% of CEOs are increasing spending on technology, data, and IT (including AI), only 28% are boosting funding for essential security and risk measures (see Figure 1).[1] This disparity indicates that critical areas such as governance frameworks, automated policy enforcement (policy-as-code), AI oversight, and security programs are at risk of being underfunded, which creates big obstacles to scaling AI initiatives safely.

Low readiness to address major AI disruptions. The largest readiness gap relates to AI industrialization. While 77% of CEOs identify AI industrialization as a high- to medium-impact force through 2027, only 20% report high readiness to address it. And while 75% of CEOs identify AI competitive polarization as a high- to medium-impact factor, only 26% say they are highly ready for it. Only 37% of CEOs feel highly prepared to deal with cyber escalation, one of the most mature risk domains (see Figure 2).

Figure 2: Impact of Factors and Readiness to Address High Impact Factors



n = varies; CEOs and Senior Business Executives; excluding don't know
Q. For each factor below, how much impact do you expect it will have on your organization's strategic business objectives through 2027?
Q. For each factor you rated as "high impact," please indicate your organization's current readiness to address it.
Source: 2027 Gartner CEO Survey. Conducted April -May 2026 among 203 global CEOs and senior business executives. Fielded by Gartner using an external panel.

Strategic Decision Implications for the C-Suite

Executive leaders face a growing exposure gap between the CEO's AI transformation ambitions and the rest of the C-suite's ability to realize those goals without incurring major risks. Organizations that close this gap can accelerate AI industrialization. Those that ignore it risk creating fast-growing operational, regulatory, and cybersecurity liabilities.

Executive leaders should focus on aligning governance, operating models, AI cost management, capital allocation, and security controls before aggressively scaling AI. Algorithmic governance is critical to improve enterprise readiness for AI. Business unit leaders must have clarity that no AI pilot will receive capital allocation for enterprise scaling until the CFO, CIO, and general counsel jointly certify its cost structure, value potential, data provenance, and risk controls.

- CFOs should reassess enterprise costing.
- General counsel and other assurance leaders should assess IP liabilities.
- CIOs should mandate algorithmic accountability and ensure continuous AI access.
- CTOs should help prevent vendor lock-in and preserve sovereignty.
- CISOs should implement automated guardrails and agentic containment.

CFOs Should Reassess Enterprise Costing

It is dangerous for boards to assume that AI will immediately expand gross margins. This belief massively underestimates the cost and effort required to build the necessary infrastructure and to derisk AI systems.

While organizations calculate the cost of AI vendor licenses, they often ignore the "hidden iceberg" of AI-related costs, such as energy and hardware, data engineering, continuous model observability, workflow redesign, and compliance audits. These costs can be volatile and rapidly liquidate expected operational savings from AI. Only 45% of senior functional leaders report that they stayed on planned budget for their 2025 AI investments.[2]

- The CFO must manage AI costs strategically. For example, for any budgeted amount the CIO requests to license AI foundation models, the CFO should mandate the allocation of an appropriate percentage of funds to AI red-teaming, data sanitation pipelines, energy costs, and the continuous automated observability of AI decision making.

General Counsel and Other Assurance Leaders Should Assess IP Liabilities

Organizations often unknowingly absorb severe legal liabilities from their software ecosystem. Over 63% of enterprise software vendors advertising AI capabilities fail to disclose their AI subprocessor, some of which are third-party subprocessors, in their documentation.[3] Enterprises put value at risk when they deploy tools without knowing whose models are running under the hood, whether they infringe on copyrighted training data, and how delegated decisions are made. Legal liability may be more costly than just budget overruns.

- Review outstanding contractual terms with key vendors as part of AI risk governance. Update all procurement master agreements to mandate that vendors disclose third-party subprocessors and provide full data provenance indemnification against copyright infringements. Establish a policy for algorithmic liability, whereby autonomous decision-making tools can be audited before deployment.

CIOs Should Mandate Algorithmic Accountability and Ensure Continuous AI Access

- Implement stronger oversight before your organization accelerates AI deployment. Mandate algorithmic accountability by deploying a ”sanitized AI sandbox” or walled-off digital playground where employees can experiment with AI tools but the system has no access to real company data. This step enables your staff’s demand to use AI tools safely while your tech team takes the time to properly clean and secure your core data pipelines.
- Write contract guarantees that ensure your AI vendors will always provide the computing power and energy needed to keep your AI running. Maintain contingency plans in the event that extraterritorial actions inhibit AI access.
- Make sure the IT budget accounts for the investments needed to derisk AI systems. Regularly update the CFO concerning changing market and business conditions and funding requirements.

CTOs Should Help Prevent Vendor Lock-In and Preserve Sovereignty

- Where possible, deploy small language models directly on edge devices or localized private servers to simultaneously mitigate the data context problem, reduce the risk of hyperscaler vendor lock-in, and mitigate sovereignty issues.
- Build a “plug-and-play” system by using open tech standards and APIs so your software is not permanently glued to one specific AI model. If a vendor changes its terms, you should be able to easily swap out its AI for a competitor’s.

CISOs Should Implement Automated Guardrails and Agentic Containment

- Deploy continuous automated monitoring and guardrails to prevent agentic AI systems from making unauthorized cross-system calls or breaching network perimeters.

[1] **2027 Gartner CEO Survey — Wave 1.** This survey was conducted from 23 April to 28 May 2026 to examine CEO views on current business issues and areas of technology impact. A total of 203 CEOs and other senior business executives participated in the survey. All respondents were screened for active employment in organizations with $50 million or more in annual revenue. Participants included CEOs (n = 156); board of directors (n = 10); chairpersons (n = 1); presidents/owners/sole proprietors (n = 5); university vice chancellors, presidents, or rectors (n = 1); CFOs (n = 10); COOs (n = 9); and other C-level executives (n = 11). Participants were from the U.S. (n = 86); Europe (n = 55); the Asia/Pacific region, excluding China (n = 32); Latin America (n = 8); South Africa (n = 1); the Middle East (n = 3); and Canada and Mexico (n = 18). Organization revenue ranged from $50 million to less than $1 billion (n = 70), $1 billion to less than $10 billion (n = 99), and $10 billion or more (n = 34). Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

[2] **2026 Gartner C-Suite AI Survey.** This survey was conducted to understand how enterprises are approaching AI, including budget allocations, current state of implementation and impact, AI strategy, and use cases across key business functions. The functions covered in the survey include finance (n = 160), HR (n = 135), procurement (n = 134), supply chain (n = 135), marketing (n = 154), sales (n = 135), customer service (n = 95), IT (n = 161), product management (n = 59) and legal/risk/compliance (n = 135); legal subfunction (n = 84), compliance subfunction (n = 31). The research was conducted online from January through April 2026 among 1,303 respondents across various industries and regions, including North America (n = 671), EMEA (n = 425), Asia/Pacific (n = 141), LATAM (n = 65), and others (n = 1). Qualifying organizations reported enterprisewide annual revenue of at least $50 million (or equivalent) in fiscal year 2025. Participants were required to be either the most senior leader or one level below the most senior leader within their respective function, and have familiarity with AI strategy, implementation, and budget for that function. Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

[3] Privacy and AI Trends Report 2026: Shadow AI Emerges as a Growing Threat While Core Privacy Challenges Persist, DataGrail.

Not a client? Talk to a specialist to act fast, execute quickly and achieve your mission critical priorities.

Gartner clients can access the full journal here.

Gartner

Actionable, objective insights

Explore these additional complimentary resources and tools:

Insights
Accelerate Enterprise AI Value Realization at Scale
Learn why and how CIOs are accelerating AI value realization at scale

Download Now

CIO Insights
2027 CIO Agenda Preview
Explore benchmark data on technology investment from CIOs worldwide.

Download Now

Webinar
The Priorities Defining CIO Success for 2027
Explore insights from the Gartner 2027 CIO and Technology Executive Survey.

Watch Now

Tool
AI Use Case Insights
Discover AI opportunities tailored to your organization.

Get Started

Already a client?
Get access to even ore resources in your client portal. Log In

Connect with us

Get actionable, objective business and technology insights to deliver on your mission-critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance. Contact us to become a client:

U.S.: +1 855 811 7593

International: + 44 (0) 3330 607 044

Become a Client

Stay connected to the latest insights

Attend a Gartner conference

View Conferences

Gartner