BCG

Tech + Us

February 2026

AI Is Quietly Changing How Risk Enters the Business

As AI systems act faster and with greater autonomy, leaders must now rethink how control, accountability, and decision logic are designed into AI from the start.

AI is rewriting the cyber playbook

A global BCG survey of 500 senior leaders shows that attackers are using AI to scale vulnerability discovery and industrialize fraud at machine speed. The result is faster, more damaging breaches with real financial, operational, and regulatory consequences. Yet, while over half of executives rank AI-driven cyber risk among their top three threats, only 5% of organizations have meaningfully increased their cybersecurity investment.

60% of recent cyberattacks suggest AI involvement, but only 5% of companies have increased cyber spending significantly.

SPEED UP CYBER DEFENSE

AI agents require different governance

Autonomous systems are moving from supporting decisions to executing them across core business processes. The value is real—but so is the risk, as existing AI governance models were not built for systems that act with limited human oversight. The leaders who move ahead will be those who rethink AI governance now—before experimentation quietly becomes exposure.

The Four Components of a Risk Framework for AI Agents

- Comprehensive risk taxonomy
- Expanded test infrastructure
- Ongoing monitoring
- Robustness and resilience

SIX MUST-ASK QUESTIONS

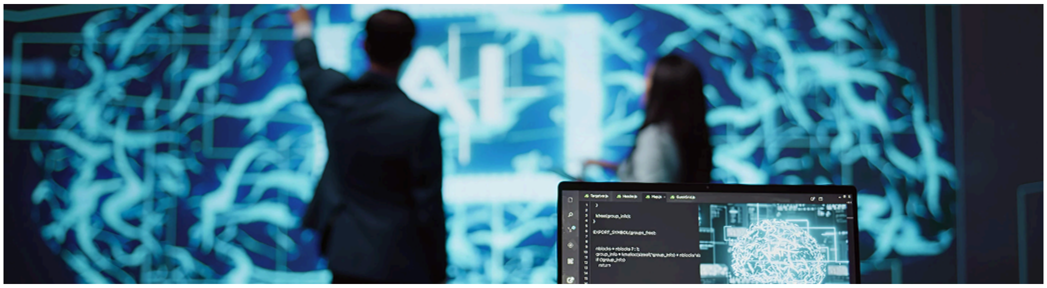
GenAI model evaluation must evolve

As GenAI moves into the core of business decision making, model selection has become a strategic choice—not a technical one. Too often, leaders rely on benchmark performance or delegate decisions entirely to experts, overlooking how each model's embedded perspective shapes outcomes. The real question for executives is not which model performs best in theory, but which perspective aligns with the company's priorities and decision logic.

Model Perspectives

- Supportive
- Adversarial
- Diverse Perspectives

ESTABLISH A MODEL EVALUATION SYSTEM



Eight Tips to Make GenAI Do What You Want

How do you get GenAI to deliver what the business actually needs? Julian King, an AI-first BCG consultant with a PhD in astrophysics, shares insights from querying GenAI chatbots up to 100 times a day. *You Are Not Hallucinating* spotlights BCG's AI experts, translating hands-on experience into practical guidance and a fresh perspective for the C-suite.

LEARN MORE

FURTHER READING

Consumers Trust AI to Buy Better. Brands Need to Move Quickly.

How Platforms Are Colliding and Why This Will Spark the Next Era of Growth

How Quantum Computing Will Upend Cybersecurity

BCG

FOLLOW US ON

Boston Consulting Group

200 Pier Four Boulevard, Boston, Massachusetts 02210, USA