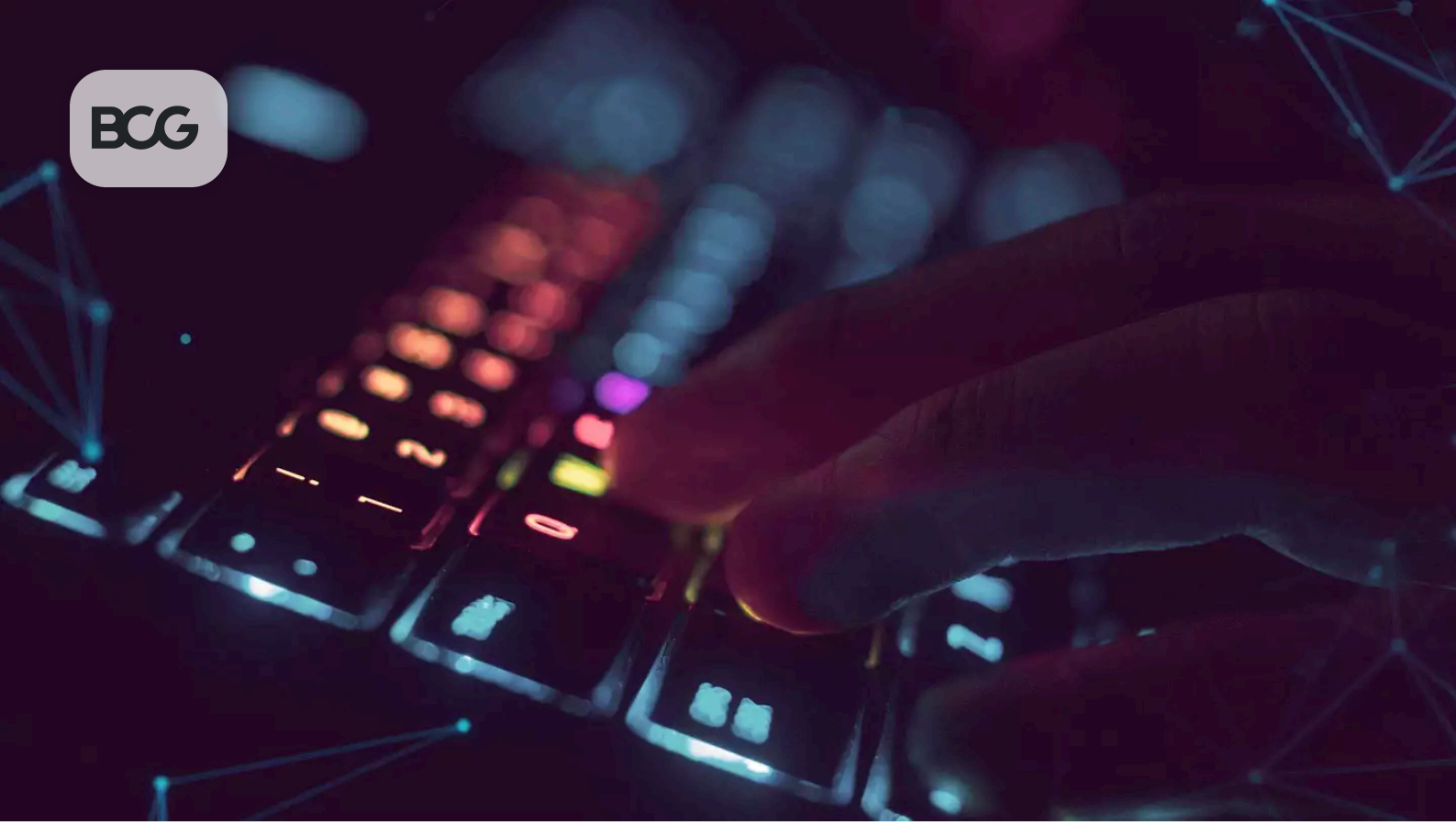


PRINCIPAL INVESTORS AND PRIVATE EQUITY

AI Creates New Cyber Risks. It Can Help Resolve Them, Too

By Braden Holstege, Clark O'Niell, Colin Troha, Vanessa Lyon, Alex Asen, Yixing Su, Sean Mitchell, Shai-Li Ron, and Helen Rhee

ARTICLE JULY 30, 2025 8 MIN READ

AI has led to a wide range of new applications and solutions to transform businesses, but for chief information security officers (CISOs) and the organizations they protect, it also creates new vulnerabilities. In fact, AI-powered attacks are now the main issue keeping CISOs up at night. As a result, companies are adjusting their cyber budgets—and in many cases incorporating AI-enabled solutions to keep their organizations, customers, and data safe.

BCG and GLC recently surveyed CISOs to understand their concerns and priorities in an ever-changing cyber risk landscape. (See “About the Survey.”) The results show that AI-powered cyber attacks have risen to become the top concern, up from fifth place last year and cited by 80% of CISOs in the survey. (See Exhibit 1.) Persistent concerns like cloud risk, third-party security, and endpoint protection continue to hold steady.

About the Survey

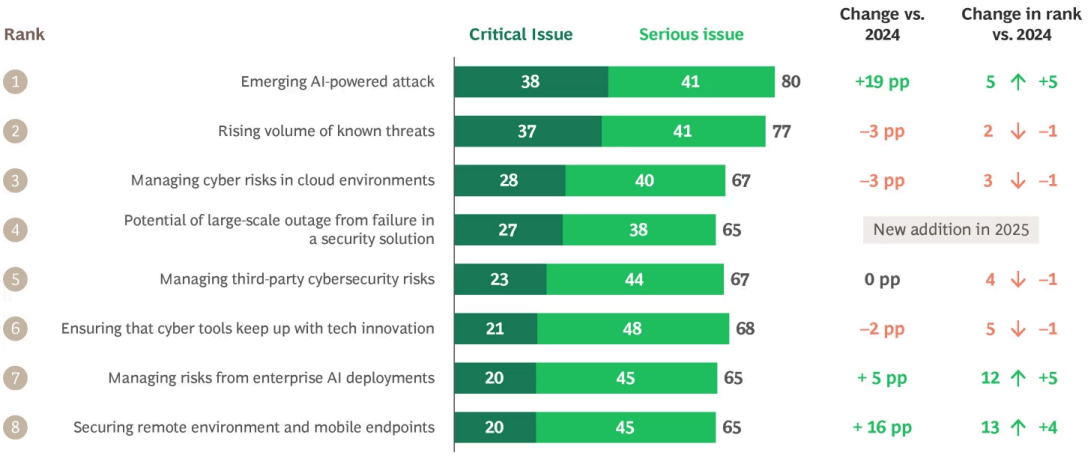
To conduct the survey, BCG’s Center for Leadership in Cyber Strategy—along with the firm’s Principal Investors and Private Equity and Telecommunications, Media, and Technology practices—recently partnered with GLG, a research firm that primarily serves the financial industry. The survey drew responses from more than 300 CISOs across geographic markets, company sizes, and industries. We also segmented respondents based on their cyber maturity to identify how leading organizations set themselves apart. (This follows similar analyses in 2024 and 2023.)

EXHIBIT 1

AI-Powered Attacks Have Become a Bigger Concern for CISOs

Top CISO Priorities (% of respondents)

Q: Please rate the importance of the below priorities on a scale from 1–5.



Source: BCG & GLG CISO Survey (April 2025, n = 300).
Note: Numbers may not sum due to rounding.

Other key findings include:

- To prepare for AI-powered attacks and evolving cyber threats, CISOs expect to continue increasing spend across cyber categories, especially in threat intelligence and application security. Overall, budgets will likely grow by about 10% this year, in line with the increase in previous years.
- CISOs are showing stronger interest in adopting new cyber features from existing vendors instead of new vendors.

Our findings have clear implications for all stakeholders. CISOs, C-suites, and boards need to remain vigilant against the growing range of cyber threats. Cybersecurity vendors need to continually refine and update their offerings. And investors need to ensure that the cybersecurity companies in their portfolio continue to develop product features and capabilities to address the changing cyber threat landscape.

The Rapid Rise of AI-Enabled Threats

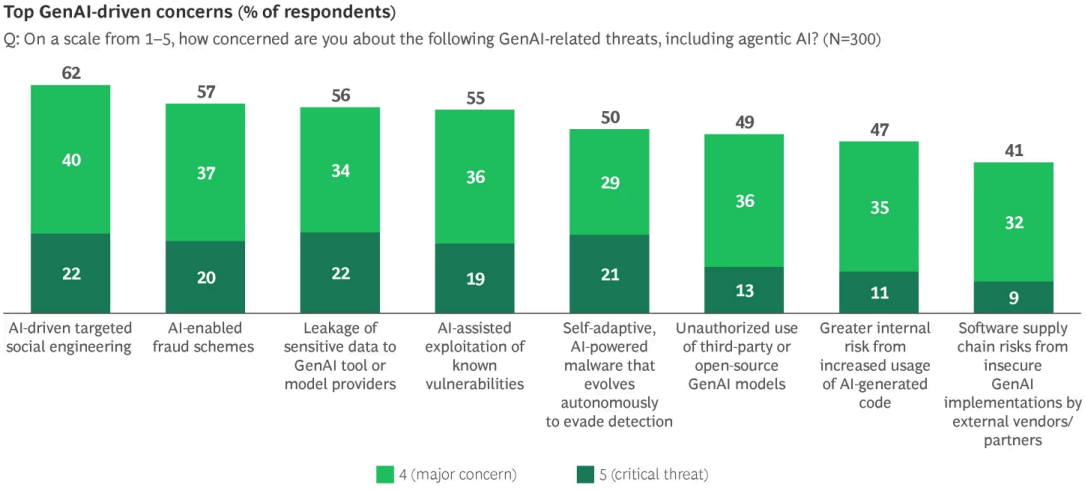
In our results for 2025, AI-powered attacks have become the top CISO concern, with a sharp 19-point increase over last year. That reflects the rapid evolution of AI overall, creating more complex and unpredictable risks that many companies are still struggling to understand.

Within GenAI, the biggest concern among CISOs are threats that exploit social engineering, cited by 62% of respondents as a major concern or critical threat. Organizations have seen a surge in automated, Gen-AI powered attacks, which are increasingly easy for attackers to execute and can be extremely effective at deceiving employees, partners, or customers. As one respondent put it, "We've seen personalized attacks, at speed and at scale, targeting both employees and customers. We know the only way this can be done is with GenAI tools."

CISOs are also highly concerned about AI-enabled fraud schemes, leakage of sensitive data during the use of GenAI tools, and AI-assisted exploitation of known vulnerabilities—all cited by more than half the CISOs in our survey. (See Exhibit 2.)

EXHIBIT 2

The Most Concerning AI-Related Threats Are Those Based on Social Engineering, Which Can Bypass Some Technical Countermeasures



Source: BCG & GLG CISO Survey (April 2025, n = 300).
Note: Numbers may not sum due to rounding.

Companies are taking action to meet the AI threat, but some are struggling to keep pace. Specifically, CISOs point to increasing investments in cyber awareness training and threat intelligence as the top two measures against GenAI threats.

Bolstering existing cyber tools with new GenAI capabilities is also a top priority. Most organizations plan to adopt GenAI-driven cyber features from existing vendors (instead of startups), with half expecting to increase their budget to adopt GenAI-cyber features and the other half expecting to adopt GenAI features within the current budget.

On the other hand, even the most cyber-mature organizations in our sample are lagging on protecting their GenAI business systems from attack, with only 30% having implemented or piloted cyber solutions specifically to protect GenAI-related systems.

Continued Changes in Product and Vendor Priorities

Looking at shifts in products and vendors, threat intelligence and application security products have become increasingly ubiqitous over the past two years. In both categories, cited adoption rates have risen from a range of 50% to 60% in 2023 to nearly 80% in 2025.

Areas like zero-trust network access, data security, identity and access management, and threat intelligence all show projected spend increases of 10% or more. Regarding threat intelligence, for example, as organizations face continued uncertainty from unknown threats (especially from GenAI), they are looking to get as much intel as possible on what might be coming their way and how to proactively defend themselves.

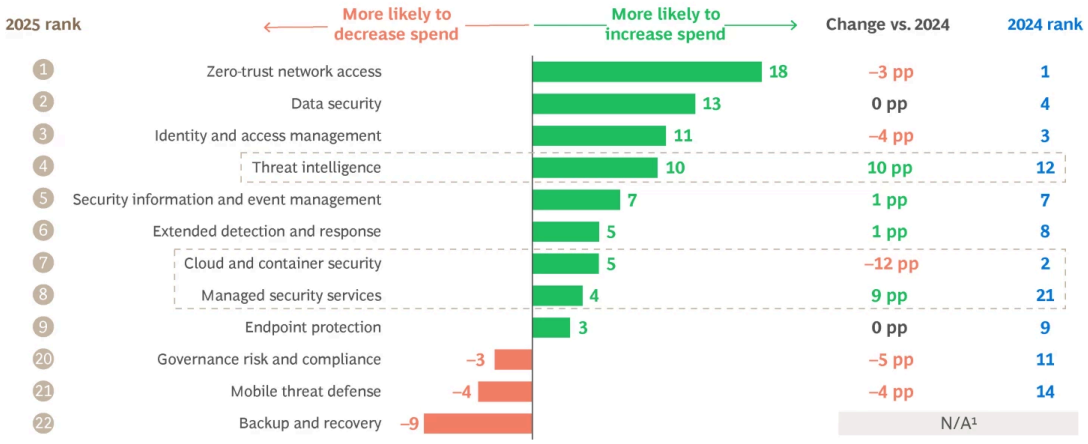
In contrast, CISOs expect to spend less on baseline services such as governance, risk, and compliance, mobile threat defense, and backup and recovery—many of which are bundled into broader offerings. (See Exhibit 3.)

EXHIBIT 3

Threat Intelligence Has Spiked in Importance Relative to 2024

Top product categories for expected spend growth (% of respondents)

Q: Please select up to 3 product categories where you expect the largest spend increases or decreases over the next year (2025 vs 2024).



Source: BCG & GLG CISO Survey (April 2025, n = 300).
Note: Percentage calculated as percent of respondents increasing spend minus percent of respondents decreasing spend.
¹Backup and recovery was newly added as a category in this iteration of the survey.

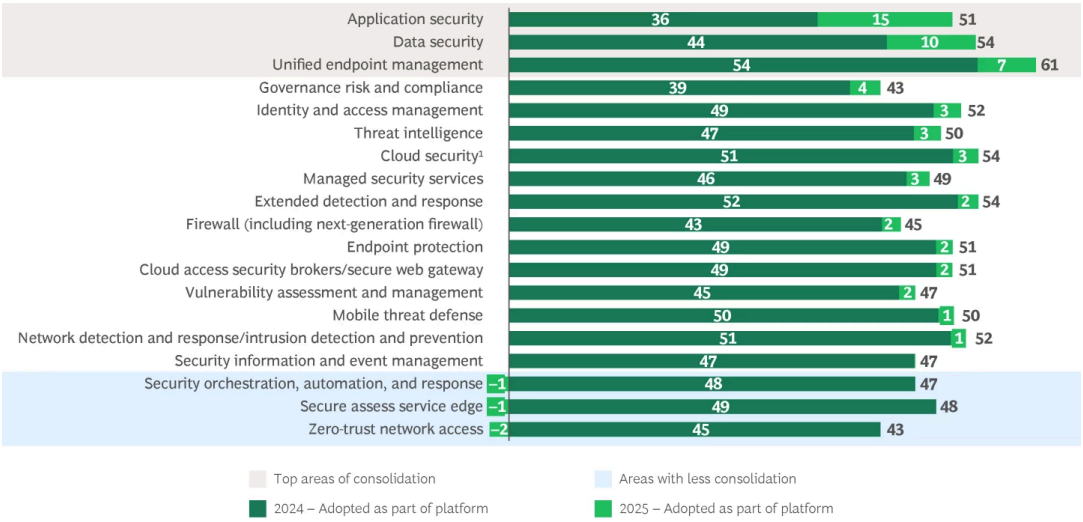
Similarly, the consolidation among vendors noted in previous years continues this year. Across most cyber product categories, far more CISOs expect to consolidate than expand vendors. Compared to the survey results last year, application security, data security, and unified endpoint management are the three product categories where CISOs expressed significantly higher interest in consolidation, potentially driven by vendors' platform strategy. (See Exhibit 4.)

EXHIBIT 4

The Consolidation Trend Continues, with CISOs Increasingly Buying Platforms Rather Than Individual Solutions

Level of platformization by product category, 2024 vs. 2025 (% of respondents)

Q: In which categories does your company adopt a best-of-breed vs. suite approach?



Source: BCG & GLG CISO Survey (April 2025, n = 300).
Note: Numbers may not sum due to rounding.
¹Cloud security posture management (CSPM)/container security/workload protection.

Spend priorities are one area where the cyber maturity gap is noteworthy. Advanced organizations in our sample tend to be more forward-looking in how they identify risks and prioritize investments. Specifically, they are focused on risks such as AI threats and evolving privacy demands, aligned with potential future threats and the evolving regulatory landscape. In contrast, less-mature organizations lag on foundational infrastructure security and undervalue areas such as multi-cloud and data center migration. (See Exhibit 5.)

EXHIBIT 5

Advanced Organizations Look Ahead to Emerging Risks, While Unprepared Organizations Focus on Legacy Challenges

Differences in prioritized drivers by maturity level

Q: On a scale from 1–5, please indicate the importance of each driver on your cybersecurity posture and spend over the next year.

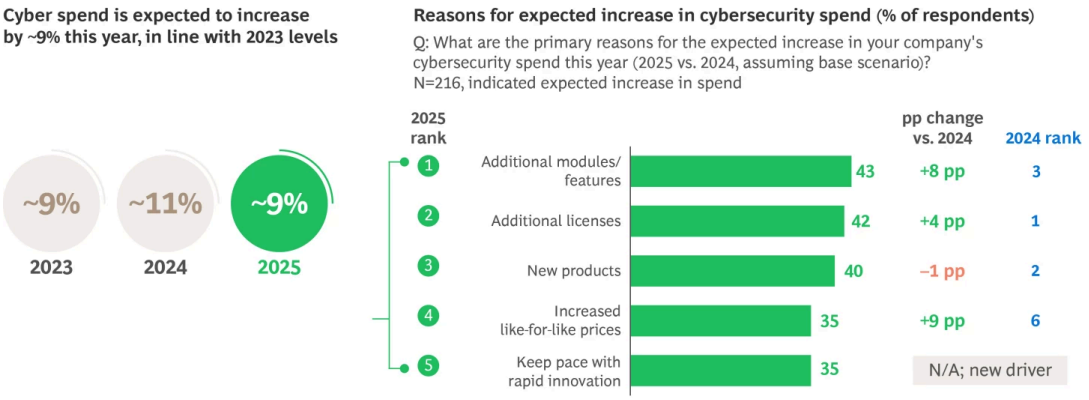
Source: BCG & GLG CISO Survey (April 2025, n=300).
Note: Response is calculated as the difference from the mean score per question, for those categorized as "advanced" vs. those categorized as "unprepared."

Growing Cyber Budgets

In a recent BCG survey of IT buyers, about one-fourth (28%) expect an overall decrease in IT budgets, primarily due to tariff-related cost pressures. Yet CISOs see cyber budgets as relatively insulated from reduction. CISOs expect cyber spend to increase by 9% in the next 12 months, slightly lower than CISOs' expectations last year (11%). (See Exhibit 6.) What's more, nearly 80% expect tariffs to have no change or only a slight shift in cybersecurity budgets.

EXHIBIT 6

Increased Cyber Budgets Are Funding the Purchase of New Modules and Features Within Existing Products



Source: BCG & GLG CISO Survey (April 2025, n=300).

There are several potential explanations for why CISOs expect cyber budgets to hold up. One is that cuts could still be coming but CISOs simply don't know about them yet. Another is that companies are taking a "wait and see" approach to cost reductions overall, especially given the uncertainty around tariffs in the first half of 2025. Yet another is that companies see the critical value of cybersecurity and are continuing to increase their investment as the threat environment escalates.

The Bottom Line for Stakeholders

Our findings have clear implications for all stakeholders in cybersecurity, from C-suites and CISOs to vendors and investors.

Priorities for CISOs, C-Suites, and Boards. Organizations, from the board to the CISO, should increasingly focus on cybersecurity outcomes. Given the evolving landscape of cyber threats, companies cannot afford to relax. That is particularly true for AI-empowered attacks, which increasingly rely on social engineering and fraud and are extremely cheap to produce convincingly and at massive volume. Although cost is a factor in assessing vendors, CISOs should focus more on cybersecurity return on investment (ROI) than price alone—and remain abreast of consolidation and other developments in the vendor landscape.

Priorities for Cybersecurity Vendors. For cybersecurity vendors, our findings underscore the importance of continually revising and upgrading their product capabilities, especially regarding GenAI-driven features. While there are still niches for point solutions to succeed, enterprise customers show a clear preference for vendor consolidation and acquiring new capabilities through add-on modules and bundles offered through current providers. Accordingly, vendors should aim to

grow through upselling and cross-selling to existing customers or attracting new customers on the strength of their overall platform.

In addition, cyber vendors should continue to emphasize the reliability and resilience of their solutions, both within their R&D and product development lifecycle and as a differentiating feature in their go-to-market strategy.

Priorities for Investors. For private equity firms that currently back cybersecurity providers—or seek to—our data shows the fundamental resilience of the sector. Economic and geopolitical uncertainty is pushing companies to scale back IT investments, but cybersecurity remains a budgetary priority. That said, investors need to make sure the cyber companies in their portfolio continue to deliver value—through factors such as the overall breadth of features, AI-related innovation, and a bedrock ability to protect companies from evolving cyber threats—rather than trying to compete on costs. Investors also need to work with their portfolio companies on how to build a marketing message around ROI to customers, to drive adoption.

The growing scope and capabilities of bad actors mean that all stakeholders—CISOs, boards, vendors, and investors—cannot rest. AI, including GenAI, is fueling a new era of cyber threats, but other developments and disruptions are coming. Our findings show the degree to which cybersecurity vendors are meeting these challenges—and the steps that CISOs are taking to keep their companies and customers safe.

Authors

Braden Holstege

Managing Director & Partner
San Francisco - Bay Area

Clark O'Niell

Managing Director & Partner
San Francisco - Bay Area

Colin Troha

Platinion Managing Director
Washington, DC

Vanessa Lyon

Managing Director & Senior Partner
New York

Alex Asen

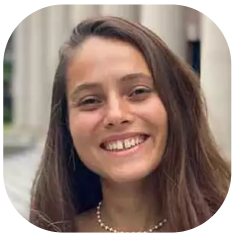
Knowledge Director
ACC – Boston

Yixing Su

Principal
San Francisco - Bay Area

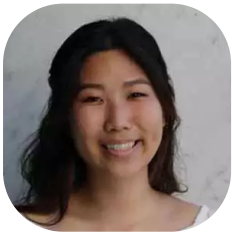
Sean Mitchell

Principal
ACC – Boston



Shai-Li Ron

Senior Associate
San Francisco - Bay Area



Helen Rhee

Senior Associate
San Francisco - Bay Area

ABOUT BOSTON CONSULTING GROUP

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders—empowering organizations to grow, build sustainable competitive advantage, and drive positive societal impact.

Our diverse, global teams bring deep industry and functional expertise and a range of perspectives that question the status quo and spark change. BCG delivers solutions through leading-edge management consulting, technology and design, and corporate and digital ventures. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, fueled by the goal of helping our clients thrive and enabling them to make the world a better place.