EXECUTIVE PERSPECTIVES ON TOP RISKS AND OPPORTUNITIES

for the Near - and Long - Term

protiviti®
Global Business Consulting

Protect, Respond, Transform:The CISO's Priorities for 2027 and Beyond

CISOs broaden their risk agenda as cyber threats, AI governance and resilience pressures intensify.

For today's CISOs, protecting the enterprise is only part of the mandate. Cyber threats, privacy obligations, artificial intelligence, regulatory change and third-party exposure all demand attention, while business leaders expect security teams to support transformation, enable growth and respond quickly when disruption occurs.

Cyber threats remain the highest-rated near-term risk, but they are increasingly interconnected with broader business concerns. AI deployments create opportunities for innovation while introducing new governance, data security and accountability requirements. Third-party relationships can expand capabilities and accelerate growth while extending risk across the enterprise ecosystem.

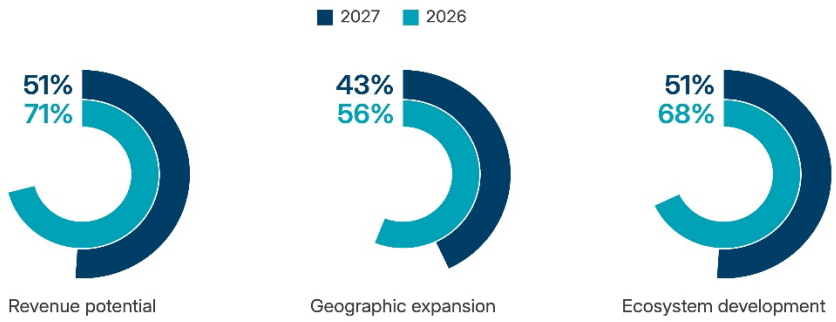
This year's Top Risks and Opportunities Survey highlights a gap between protection and agility. While 41% of CISOs express high or very high confidence in their orginisations' ability to protect enterprise value, only 29% say the same about response capabilities. Respondents are prioritisingAI governance and workforce readiness while investing in infrastructure modernisation, regulatory compliance and workforce skills.

Viewed together, the findings point to a broader and more demanding CISO agenda. CISOs are being asked not only to defend the orginisation, but also to strengthen resilience, guide the responsible adoption of emerging technologies and help the enterprise pursue transformation without taking on unacceptable risk.

Where do CISOs see the greatest opportunities for their orginisation over the next two to three years?

For CISOs, growth remains important over the next two to three years, but their outlook is notably more cautious than it was a year ago. Optimism declined across all three opportunities assessed in the survey. Agreement on revenue potential fell from 71% to 51%, ecosystem development from 68% to 51%, and geographic expansion from 56% to 43%. Disagreement increased in every category.

Views about opportunities for growth – CISOs



Based on a five-point scale assessing agreement/disagreement.
Percentages reflect sum of “Agree completely” and “Agree somewhat” responses.

The results do not necessarily indicate fewer technology-enabled paths to growth. Rather, they reflect an operating environment shaped by limited economic growth, geopolitical uncertainty and constrained budgets. Orginisations continue to expect cybersecurity and technology teams to support expansion and innovation, often without providing additional resources. For CISOs, the question is increasingly which opportunities the enterprise can pursue securely and resiliently within its existing capacity.

Revenue potential and ecosystem development remain the strongest opportunities, with 51% of respondents agreeing that each will be significant. Supporting revenue growth requires CISOs to identify security, privacy and resilience requirements early enough to inform business decisions — not after a new product, service or market strategy is underway. Early

involvement allows security to enable disciplined growth while helping leaders understand the exposure associated with competing investments.

Geographic expansion presents additional complexity. New markets can open revenue streams but also introduce regulatory fragmentation, data sovereignty requirements and geopolitical risk, making consistent security and governance practices more difficult to maintain.

Ecosystem development can accelerate transformation by providing capabilities that would be costly or time-consuming to build internally. Yet every partner and platform expands the orginisation's dependency network and raises questions about data access, identity, operational resilience and third-party risk.

CISOs are not rejecting growth. They are applying greater discipline to how it is pursued. Involving them early in market, partnership and operating-model decisions can help orginisations build security and resilience into growth strategies from the outset.

What priorities do leaders see as most important to maximisingthe value of AI deployments?

For CISOs, the AI conversation is shifting from adoption to controlled value creation. The question is no longer whether orginisations will use AI, but how they can realise its benefits without allowing deployment to outpace governance, security and accountability.

The findings reflect that priority. Improving governance and accountability leads at 51%, followed by equipping the workforce to realise AI's value at 45% and integrating AI with existing technologies, business processes and employees at 32%. By comparison, only 13% selected deploying AI at a more competitive pace as a top-three priority.

The emphasis on governance is telling. For CISOs, governance extends beyond compliance. It defines who owns AI systems, which uses are permitted, what data they can access and who remains accountable for their actions. These questions become more complex as orginisations introduce agentic AI and nonhuman identities. Effective guardrails can help the business accelerate adoption without creating risks that security teams must address later.

51%

rank improving governance and accountability for AI deployments as a top priority.

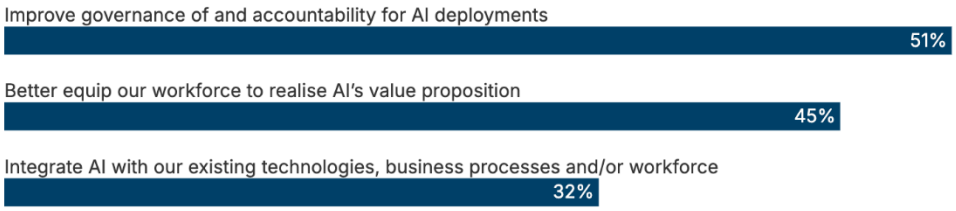
Integration also matters. AI is more likely to deliver value when it improves existing technologies, processes and workflows rather than operating as a stand-alone initiative. However, deeper integration expands the points at which AI can access data, influence decisions or initiate actions. CISOs need visibility and controls that remain effective as deployments scale.

Workforce readiness is equally critical. Employees must understand how to use AI appropriately, assess its outputs and recognise risks involving inaccurate results, bias, data exposure and misuse.

Data security ranked lower than expected, at 26%, but that result does not suggest indifference. Respondents could select only three priorities, and many may view data protection as one component of the broader governance challenge.

CISOs are not seeking to slow AI adoption. They are focused on enabling controlled, secure growth. Orginisations that build governance, workforce readiness, integration and security into adoption from the outset will be better positioned to realise sustainable value.

Top AI opportunities – CISOs



We asked CISOs three specific questions about their views on the orginisation's ability to (1) transform the enterprise, (2) protect enterprise value, and (3) respond with agility to market opportunities and risks. What did they tell us?

For CISOs, the findings reveal a clear divide between protecting enterprise value and responding when threats or disruptions occur. Confidence is highest in Protect, with 41% reporting high or very high confidence, followed by Transform at 38%. Respond trails at 29%, with 54% expressing only moderate confidence. The results suggest that established controls are



easier to manage than the cross-functional demands of containing an incident and restoring operations.

The relative confidence in protection reflects the traditional focus of the CISO role. Orginisations have invested heavily in cybersecurity controls, threat detection and vulnerability management. Yet breaches are increasingly viewed as inevitable, and frontier AI may make attacks faster and more difficult to contain. Prevention remains essential, but resilience also depends on limiting losses and restoring critical operations quickly.

Respond presents a different challenge because much of it falls outside the security function's direct control. Recovery may require technology teams to restore systems, business leaders to prioritize operations, legal and communications teams to manage external obligations, and third parties to address disruptions. Confidence can suffer when these groups have not tested their ability to operate together under pressure.

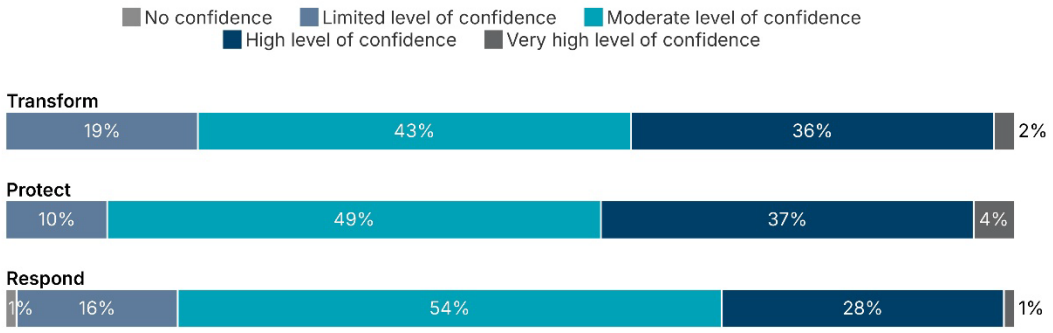
Testing practices may contribute to the gap. Many orginisations conduct penetration tests, but fewer perform red-team exercises, and fewer still use blue-team exercises to demonstrate that defenders can detect, contain and recover from an attack. Tabletop exercises support planning but do not necessarily prove operational readiness.

Transformation can help bridge protection and response. Automation, modern infrastructure and redesigned processes can reduce routine workloads and redirect capacity towards emerging risks. For boards, the central question is not simply whether controls exist. It is whether the enterprise can coordinate decisions, contain disruption and recover when those controls fail.

54%

Express only a moderate level of confidence in the orginisation's ability to respond with agility to market opportunities and risks.

Views about the ability to transform, protect and respond – CISOs



AI's greatest opportunity lies in disciplined value creation built on strong governance, workforce readiness, secure integration and accountability.

What are the most significant near-term concerns and risks on the minds of CISOs?

If there is a common thread running through the CISO rankings, it is convergence. Cybersecurity, privacy, economic pressure, third-party exposure and AI risk increasingly reinforce one another. A cyber incident can trigger privacy and regulatory consequences. An AI deployment can expand data, identity and third-party risks. Economic constraints can delay modernisation and limit response capacity. For CISOs, these concerns rarely exist in isolation.

Top five near-term risks

CISO

Question	2027	2026
Cyber threats	3.54	3.36
Ensuring privacy and compliance with growing identity protection regulations and expectations	3.39	2.81
Economic conditions, including inflationary pressures	3.31	2.59
Third-party risks	3.28	3.17
Emergence of new risks from implementing artificial intelligence	3.28	2.99
Resiliency and/or agility to manage an unexpected crisis and other uncertainties	3.28	2.48

Cyber threats remain the leading concern, rising from 3.36 to 3.54. As attacks grow faster and more sophisticated, orginisations must strengthen prevention while improving their ability to limit losses and restore operations.

Privacy ranks second, increasing from 2.81 to 3.39. Requirements in California, the European Union and other jurisdictions, combined with scrutiny of cross-border data sharing, are making compliance more complex. Expanding AI use further increases the data accessed by employees, systems and third parties.

Economic conditions rank third, rising from 2.59 to 3.31. Limited growth and constrained budgets are forcing security teams to meet rising expectations with the same or fewer resources, potentially slowing modernisation and resilience initiatives.



Third-party risk and AI implementation risk each scored 3.28. Orginisations increasingly depend on vendors, platforms and ecosystem partners, extending exposure beyond their direct control. Agentic AI and nonhuman identities also create unresolved questions about authorisation, accountability and data access.

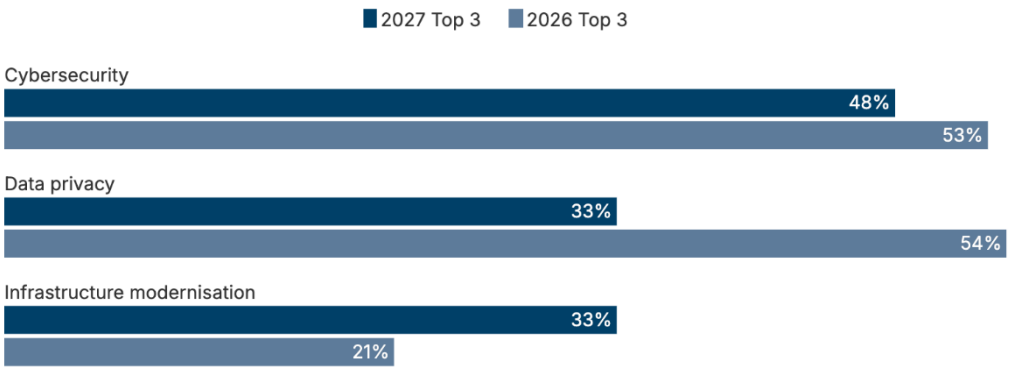
Resilience and regulatory uncertainty also scored 3.28, underscoring the tightly clustered risk landscape. The challenge is not managing one dominant threat. It is building an orginisation that can understand interconnected risks, adapt controls and recover quickly when disruption occurs.

The bottom line: The results are less about one dominant risk than the convergence of cyber, privacy, economic, third-party and AI concerns. For CISOs, the challenge is no longer simply defending against individual threats. It is building an orginisation that can understand interconnected exposures, quantify their potential business impact, adapt controls as conditions change and recover quickly when disruption occurs.

Given these near-term risk issues, where do orginisations plan to invest most?

CISOs appear to be rebalancing investment towards capabilities that can strengthen security, modernisation and regulatory readiness at the same time. Cybersecurity remains the leading priority, but the year-over-year results suggest that flat budgets and expanding demands are forcing orginisations to make limited resources work harder.

Top strategic investment priorities – CISOs



48%

rank cybersecurity as a top strategic investment priority.

Cybersecurity ranks first for 2027, selected by 48% of respondents, down from 53% in 2026. The decline does not indicate that cyber risk is receding; cyber threats remain the leading near-term concern. Instead, CISOs are being asked to address evolving threats, AI adoption and operational complexity without corresponding budget increases.

Data privacy and infrastructure modernisation tie for second at 33%. Data privacy led all investment areas in 2026 at 54%, making its 21-point decline particularly striking as privacy rises to the second-highest near-term risk. Some privacy funding may be shifting into broader data governance, AI governance, modernisation and compliance initiatives. Orginisations should confirm, however, that privacy capabilities are embedded in those programmes rather than losing ground to competing priorities.

Infrastructure modernisation increased from 21% in 2026 to 33% in 2027. Modernisation can reduce technical debt and the attack surface, strengthen identity and access controls, improve visibility and support automation. It also can release resources currently devoted to maintaining legacy environments.

The 2026 top three were data privacy at 54%, cybersecurity at 53% and regulatory compliance infrastructure at 26%. The 2027 results signal a shift towards foundational capabilities that can support several risk outcomes.

The bottom line: CISOs are not stepping back from protection. They are redirecting limited resources towards a more modern, scalable security foundation. The challenge is ensuring that cyber, privacy and compliance outcomes remain fully funded as investment moves towards transformation.

How do CISOs view the 10-year risk outlook for their orginisation?

Over the next 10 years, CISOs are focused on securing increasingly digital, interconnected and automated operations. The priority is building security programmes that evolve with technology, workforce needs and business models.

Security and privacy remain the leading long-term risk theme, selected by 49% of CISOs, down from 64% in 2026. The decline likely reflects a broader agenda in which these concerns are embedded in AI, workforce, third-party



and resilience initiatives. Their prominence across both time horizons confirms they remain enduring enterprise priorities.

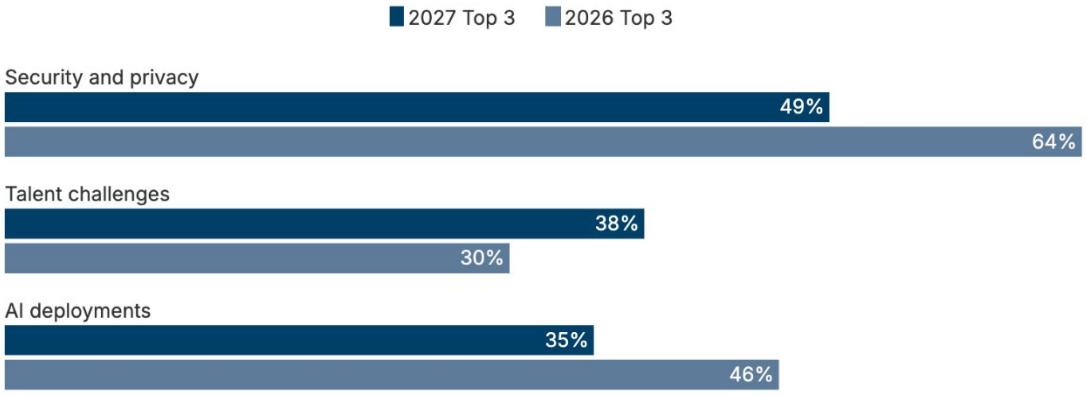
Talent challenges rank second, rising from 30% to 38%. Orginisations need professionals who can secure emerging technologies, govern AI, modernise identity and access controls, manage third-party exposure and maintain legacy systems. CISOs must build teams with the technical, business and risk skills to navigate a rapidly evolving threat landscape.

AI deployments rank third at 35%, down from 46% in 2026, suggesting AI is shifting from a discrete future concern to a current operating reality. Its long-term implications span data governance, nonhuman identities, workforce readiness, resilience and third-party risk.

In 2026, the top three risks were security and privacy at 64%, AI deployments at 46%, and markets and economies at 45%. The 2027 ranking — security and privacy, talent challenges, and AI deployments — shifts the emphasis to the people, governance and controls required for sustained technological change.

The bottom line: Long-term resilience requires skilled people, adaptable governance and controls that evolve with increasingly interconnected risks.

Top long-term risks – CISOs



Calls to action for CISOs

- **Integrate cyber risk into enterprise risk management.** Quantify potential losses and use the results to guide priorities and investments.
- **Strengthen incident response and recovery.** Test cross-functional execution through realistic red-team, blue-team and recovery exercises.
- **Clarify incident-response responsibilities.** Establish decision rights and escalation paths across security, IT, business functions and critical third parties.
- **Modernise infrastructure and security architecture.** Reduce technical debt and the attack surface while improving visibility, automation, identity controls and resilience.
- **Establish AI governance before deployments scale.** Define approved uses, data-access controls, human oversight and accountability for AI-enabled actions.
- **Prepare for agentic AI and nonhuman identities.** Control what autonomous systems can access, decide and execute.
- **Protect sensitive data and prepare employees to use AI securely.** Strengthen data controls while building awareness.
- **Strengthen third-party oversight.** Assess critical partners' security and resilience, and test contingency and exit plans.
- **Reallocate resources towards transformation.** Use modernisation, automation and process redesign to create capacity for emerging risks without weakening core controls.
- **Develop the cybersecurity workforce.** Build skills in AI governance, cloud security, identity, resilience and cyber-risk quantification.
- **Measure preparedness and balance innovation with controlled growth.** Track control effectiveness, response performance and recovery outcomes while ensuring transformation does not outpace governance and oversight.



About the survey

Our 15th annual **Executive Perspectives on Top Risks and Opportunities Survey** contains insights from 1,330 board members and C-suite executives around the world regarding their views on:

- Ability to transform and protect the enterprise and respond to market opportunities and risks;
- Opportunities for growth considering the current environment;
- Priorities perceived as most critical to maximizing the value of AI deployments;
- The top risks on the horizon for the near-term (two to three years ahead) related to 30 specific risks across three dimensions (transform, protect and respond);
- A discussion of their orginisations' near-term strategic investment priorities, given the opportunities and the risks they face; and.
- The long-term horizon based on 11 risk themes that encompass the 30 near-term risk issues.

Our survey participants shared their views through an online survey conducted in June and July 2026. This paper offers specific insights into these issues from the perspective of CISOs.

About the authors



Kim Bozzella is a managing director and global leader of Protiviti's CIO & CISO C-Suite Solutions. She advises technology executives on their most critical priorities, including technology strategy and architecture, enterprise platforms, data and analytics, operating model evolution and IT value realisation. Previously, she served as the global leader of Protiviti's Technology Consulting solutions.

Contact Kim at kim.bozzella@protiviti.com.



Scott Laliberte is a managing director in Protiviti's Technology Consulting practice, serving as a trusted CISO adviser to boards and executive leadership teams. He specialises in helping orginisations understand and manage cybersecurity risk in the context of business strategy, enabling innovation while safeguarding enterprise value. Previously, Scott led Protiviti's Global Cybersecurity practice, Emerging Technology practice and attack and penetration labs

Contact Scott at scott.laliberte@protiviti.com.

Protiviti (www.protiviti.com) is a global consulting firm that helps clients transform and protect their businesses, and respond to planned and unexpected events. Through a network of more than 90 offices in over 25 countries, Protiviti and its independent and locally owned member firms deliver deep expertise and tailored capabilities across technology, artificial intelligence, data, operations, finance, legal, compliance, HR, marketing, digital, risk, and internal audit—enabling orginisations to accelerate innovation, navigate risks and safeguard what matters most.

Named to the Fortune 100 Best Companies to Work For® list since 2015, Protiviti Inc. has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti Inc. is a wholly owned subsidiary of Robert Half (NYSE: RHI).

© 2026 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans.
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. 1026

protiviti®