2026 EDITION

EXECUTIVE PERSPECTIVES ON TOP RISKS AND OPPORTUNITIES

protiviti®
Global Business Consulting

2026 CISO Outlook: Top Risks, AI Challenges, and Growth Opportunities in Cybersecurity

By Sameer Ansari
Global CISO Solutions Leader

Successful companies view even challenging times as catalysts for innovation and growth, actively seeking opportunities where others see obstacles.

Over the last 13 years, we have issued annual research reports on the top risks faced by leaders all over the world. This year, we have added an emphasis on opportunities to set the tone for identifying and responding proactively to emerging trends, market shifts and evolving customer expectations. Organizations balancing risk management with a strong focus on seeking growth are better equipped to innovate products and services, enhance their resilience, adapt to change, and achieve top-line growth and strategic differentiation. It is all about unlocking opportunity.

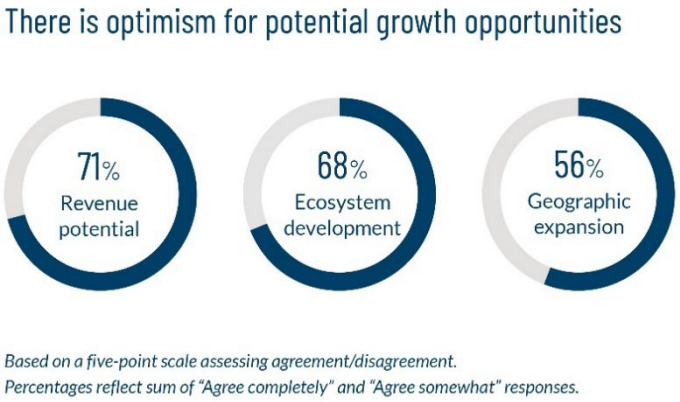
Our 14th annual Executive Perspectives on Top Risks and Opportunities Survey contains insights from 1,540 board members and C-suite executives around the world regarding their views on:

- Three specific areas for growth considering the current environment;
- Opportunities and challenges associated with the transformative impact of artificial intelligence (AI) on their organizations;
- The top risks on the horizon for both the near-term (two to three years ahead) and the long-term (a decade from now), related to 28 specific risks across three dimensions: macroeconomic, strategic and operational; and
- A discussion of their organizations' near-term strategic investment priorities, given the opportunities and the risks they face.

Our survey participants shared their views through an online survey conducted from early September through mid-October 2025. This paper offers specific insights into these issues from the perspective of the CISO (Chief Information Security Officer).

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

Over the next two to three years, Chief Information Security Officers (CISOs) are positioned to capitalize on a unique convergence of challenges and opportunities, as organizations navigate the evolving landscape of cyber risk, third-party dependencies, and rapid advances in artificial intelligence (AI). Recent research underscores a strong sense of optimism for growth, with 71% of leaders seeing revenue potential, 68% expecting ecosystem development, and 56% anticipating geographic expansion.



One of the most significant opportunities lies in elevating cybersecurity from a technical function to a strategic business driver. Increasingly, board members and executives expect CISOs to frame cyber risk in business terms and align security initiatives with organizational objectives. This shift enables security leaders to influence investment decisions and foster resilience, positioning cybersecurity as a source of competitive advantage rather than a cost center.

AI is another area where CISOs see transformative potential. While AI expands the attack surface, it also offers powerful tools for defense. Security teams are leveraging AI to automate threat detection and response, enabling faster and more effective mitigation of risks. Additionally, AI allows organizations to optimize limited resources, respond to incidents with greater agility, and address the risks associated with "shadow AI" by improving data governance and ensuring secure deployment of AI technologies.

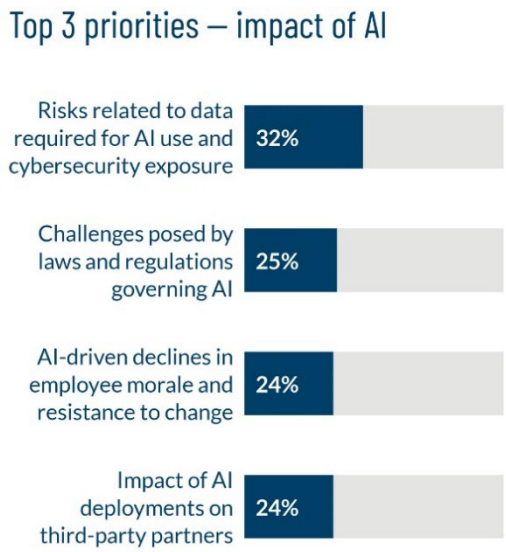
The growing reliance on third-party vendors and global supply chains presents both risk and opportunity. CISOs are moving beyond traditional compliance approaches, developing deeper risk insights, and implementing robust assessment frameworks. By fostering a "trust but verify" culture, organizations can ensure that third-party relationships strengthen, rather than compromise, their security posture.

Building organizational resilience and trust is also a top priority. Investments in cyber resiliency are aimed not only at preventing breaches but also at ensuring rapid recovery and business continuity. Maintaining customer trust through strong data protection and transparent security practices is essential for sustaining growth and competitive differentiation.

In summary, CISOs view the coming years as a time to lead security-driven innovation, harness AI responsibly, and embed cyber risk management into business strategy. By turning risk into opportunity and resilience into a differentiator, organizations are well-positioned to realize their growth ambitions.

What will be the organization's most significant challenges regarding the impact of AI over the next two to three years?

Over the next two to three years, organizations are expected to encounter a range of significant challenges stemming from the impact of artificial intelligence (AI), particularly from the perspective of the Chief Information Security Officer (CISO). The most prominent concern centers on risks related to data required for AI use and the resulting cybersecurity exposure. According to recent research, 32% of leaders identify this issue as their top priority. The widespread adoption of AI tools, including those deployed outside traditional IT oversight—often referred to as "shadow AI"—creates new avenues for sensitive data to be accessed, processed, or exfiltrated in unforeseen ways. Addressing these risks will require organizations to implement robust data governance frameworks, enforce strict access controls, and maintain continuous monitoring of AI endpoints and agents.



Another major challenge involves navigating the evolving landscape of laws and regulations governing AI. With 25% of respondents highlighting regulatory compliance as a top concern, organizations must remain agile and proactive in operationalizing policy, ensuring transparency, and maintaining regulator-ready documentation and playbooks. Collaboration among security, legal, and risk teams will be essential to keep pace with shifting requirements and to demonstrate compliance to regulators and stakeholders.

The workforce dimension also presents notable challenges. AI is transforming job designs, automating entry-level tasks, and introducing non-human identities at scale. Twenty-four percent of leaders are concerned about AI-driven declines in employee morale and resistance to change. Organizations must invest in upskilling and reskilling initiatives, communicate the value of security and AI in business terms, and ensure teams are equipped to work alongside AI—transitioning from traditional roles to AI-assisted analysts.

Finally, the impact of AI deployments on third-party partners is a growing risk, also cited by 24% of leaders. As organizations increasingly rely on external vendors for AI capabilities, new vulnerabilities are introduced. To address these risks, organizations must move beyond checkbox assessments and adopt continuous validation and "trust-but-verify" approaches for all partners.

In summary, organizations must balance innovation with robust risk management, focusing on data security, regulatory compliance, workforce adaptation, and third-party oversight to successfully navigate the challenges posed by AI in the near term.

What are the most significant short-term (two to three years) concerns and risks on the minds of CISOs?

Top global near-term risks

2026 rank	Risk issue	Average*
1	Cyber threats	3.36
2	Third-party risks	3.17
3	Emergence of new risks from implementing AI	2.99
4	Operations and legacy IT infrastructure unable to meet performance expectations	2.89
5	Adoption of new and emerging technologies elevating the need to upskill/reskill our workforce	2.83

* Average based on a five-point scale where 1 reflects "No impact at all" and 5 reflects "Extensive impact."

In the short term—over the next two to three years, Chief Information Security Officers (CISOs) are focused on a set of critical concerns and risks that reflect both the evolving threat landscape and the rapid pace of technological change. According to recent research, the top global near-term risks for CISOs include cyber threats, third-party risks, the emergence of new risks from implementing artificial intelligence (AI), challenges with operations and legacy IT infrastructure, and the need to upskill or reskill the workforce due to new and emerging technologies.

Cyber threats are the foremost concern, with an average impact score of 3.36. The expansion of digital operations, cloud adoption, and AI-powered tools has increased the attack surface, making organizations more vulnerable to sophisticated and automated attacks. CISOs are prioritizing proactive monitoring, advanced threat intelligence, and rapid incident response to build resilience against these threats.

Third-party risks, with an average score of 3.17, are also prominent. As organizations deepen their reliance on external vendors, cloud providers, and strategic partners, the complexity of the risk profile grows. The weakest link in the supply chain can expose the organization to significant vulnerabilities. Continuous assessment, robust due diligence, and "trust-but-verify" approaches are essential for safeguarding the extended ecosystem.

The emergence of new risks from implementing AI (2.99) is a rapidly growing challenge. AI introduces novel vulnerabilities, such as shadow deployments, data governance gaps, and adversarial attacks on models. CISOs must collaborate with technology teams to ensure responsible AI adoption, with clear policies, oversight, and technical controls.

Operations and legacy IT infrastructure unable to meet performance expectations (2.89) present another pressing issue. Technical debt and outdated systems can hinder agility and expose organizations to risk.

Modernization efforts must be balanced with security, ensuring that new platforms are resilient and legacy systems are adequately protected.

Finally, the adoption of new and emerging technologies (2.83) elevates the need to upskill and reskill the workforce. Talent shortages and resistance to change can slow progress and introduce risk. Investing in training and fostering a culture of continuous learning are critical to success.

Collectively, these risks demand vigilance, adaptability, and collaboration across security and technology leadership to navigate the interconnected challenges of the near term.

In summary, the next few years will demand vigilance, adaptability, and collaboration across security and technology leadership to navigate these interconnected risks.

Based on these near-term risk issues, in what areas is the organization likely to invest the most over the next two to three years, and why?

In response to escalating near-term risks, organizations are prioritizing investments in three key areas over the next two to three years: data privacy, cybersecurity, and regulatory compliance infrastructure. According to recent research, 54% of leaders identify data privacy as a top investment area, closely followed by cybersecurity at 53%, and regulatory compliance infrastructure at 26%.

Data privacy is receiving significant attention due to the proliferation of artificial intelligence, cloud computing, and digital transformation initiatives. These trends have resulted in sensitive data being more widely distributed and exposed, increasing the risk of unauthorized access or breaches. To address these concerns, organizations are investing in robust data governance frameworks, advanced encryption technologies, and continuous monitoring solutions. The objective is to embed privacy by design into all systems and processes, ensuring that data protection is not an afterthought but a foundational element of organizational trust and customer confidence.

Cybersecurity remains a central focus as cyber threats continue to dominate the risk agenda. Investments in this area are aimed at strengthening both foundational controls and advanced capabilities. Organizations are modernizing their security operations centers, leveraging AI and machine learning for enhanced threat detection and response, and building resilience against ransomware, supply chain attacks, and vulnerabilities associated with legacy infrastructure. The strategic goal is to shift from a reactive defense posture to proactive risk management, enabling organizations to anticipate and mitigate threats before they materialize.

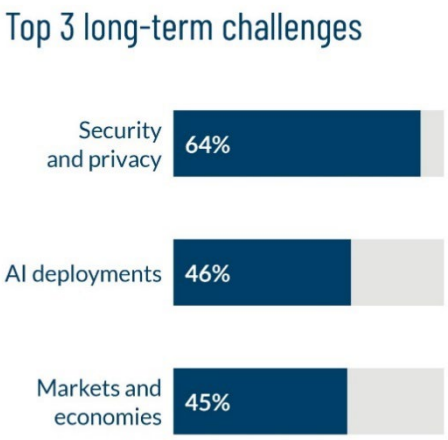
The evolving regulatory environment is driving increased investment in compliance infrastructure. With 26% of leaders prioritizing this area, organizations are preparing for new and changing laws governing data, AI, and digital operations. Investments include automation of compliance processes, policy management systems, and audit readiness tools. Collaboration between security, legal, and risk management teams is essential to ensure organizations remain compliant and can demonstrate their adherence to regulatory requirements.

Collectively, these investment priorities reflect a strategic approach to safeguarding data, defending against sophisticated threats, and ensuring compliance in a dynamic environment. Rather than serving solely as risk mitigation measures, these efforts are foundational to enabling innovation, sustaining long-term growth, and maintaining stakeholder trust in an increasingly complex digital landscape.

In summary, investments will be driven by the imperative to safeguard data, defend against sophisticated threats, and ensure compliance in a dynamic environment. These efforts are not just about risk mitigation—they are foundational to enabling innovation and sustaining long-term growth.

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

Looking out over the next decade, CISOs see a risk landscape that is both more complex and more consequential than ever before. Our research shows that 64% of leaders identify security and privacy as the top long-term challenge. This is no surprise—cyber threats are evolving, attack surfaces are expanding, and the stakes for data protection and trust continue to rise. Over the next ten years, our organizations will need to invest in advanced security architectures, privacy-by-design principles, and continuous monitoring to stay ahead of adversaries and regulatory demands.



AI deployments are the second most significant long-term concern, cited by 46% of respondents. The rapid adoption of AI will fundamentally reshape how we operate, but it also introduces new risks—from model vulnerabilities and data governance gaps to ethical dilemmas and regulatory uncertainty. As CISOs, we must ensure that AI is deployed responsibly, with robust controls, transparency, and ongoing oversight. This means working closely with technology, legal, and risk teams to build frameworks that support innovation while safeguarding the organization.

Markets and economies round out the top three long-term challenges, with 45% of leaders highlighting this area. Economic volatility, shifting global dynamics, and competitive pressures will require organizations to be agile and resilient. For CISOs, this means aligning security strategy with business objectives, supporting growth initiatives, and ensuring that risk management is integrated into every aspect of decision-making.

In summary, the 10-year outlook demands that CISOs lead on security and privacy, guide responsible AI adoption, and enable the organization to thrive in uncertain markets. Our role will be to anticipate emerging risks, foster a culture of resilience, and ensure that trust remains at the core of everything we do. The organizations that succeed will be those that treat risk management as a strategic enabler, not just a defensive necessity.

Guidance/call to action for next two to three years

Today, technology underpins nearly every business decision. The challenge for technology leaders is to turn risks and opportunities into blueprints for enterprise transformation and growth. Our call to action:

- **Translate cybersecurity into business value.** Shift from technical framing to strategic impact to influence investments and position security as a competitive advantage.
- **Strengthen data governance for AI and prepare for expanding AI regulation.** Prioritize controls that reduce exposure from AI-related data use, including shadow AI and model risks. Build agile compliance processes, documentation, and cross-functional alignment to keep pace with evolving laws.
- **Deepen third-party oversight.** Replace checkbox compliance with continuous validation and trust-but-verify assessment of vendors and partners.
- **Modernize legacy infrastructure and invest in resilience and rapid recovery.** Address technical debt and performance gaps that increase risk and slow security response. Enhance monitoring, threat intelligence, and incident response to counter expanding attack surfaces.
- **Upskill and reskill the workforce.** Support teams as roles shift alongside AI adoption; ensure analysts are prepared to operate with AI-assisted tools.

About the author

Sameer Ansari is Protiviti's Global CISO Solutions Leader. He brings more than 20 years of experience developing and delivering complex privacy solutions to the financial industry, and privacy consulting and implementation experience in the technology, media and telecommunications and consumer products industries, in many locations throughout the globe.

Contact Sameer at sameer.ansari@protiviti.com