
# 2025 Report on Top Risks for CIOs and CTOs

*By Kim Bozzella*
*Global Leader, Technology Consulting, Protiviti*

Boards of directors and senior executive teams face a complex web of uncertainties. These may generate opportunities for strategic advantage or risks leading to unexpected disruption and performance shortfalls. An ability to anticipate risks that may be on the horizon before they become imminent can help leaders navigate unfolding developments – particularly those that are uncontrollable – that may impact their organization's value and growth objectives.

Our 13th annual **Executive Perspectives on Top Risks Survey** contains insights from 1,215 board members and C-suite executives around the world regarding their views on the top risks they see on the near- and long-term horizon. Specifically, our global respondent group provided their perspectives about the potential impact over the near-term (two to three years ahead) and long-term (over the next decade) of 32 risk issues across these three dimensions:

- **Macroeconomic risks** likely to affect their organization's growth opportunities
- **Strategic risks** the organization faces that may affect the validity of its strategy for pursuing growth opportunities
- **Operational risks** that might affect key operations of the organization in executing its strategy

## Overview of near-term top risk issues in 2025

Businesses today face a myriad of challenges as they adapt and transform their operational models to overcome future obstacles, including competitive pressures and cyber threats. The global marketplace is deeply influenced by advancements in technology, changing regulations, and economic factors, all of which necessitate access to skilled professionals and expertise. These factors shape the risk landscape for CIOs and CTOs, according to our latest Top Risks Survey.

For CIOs and CTOs, near-term risks are increasingly defined by people-centric and economic issues. The availability and costs of qualified labour, inflationary pressures, expertise in emerging technologies, and the ability to counter cyber threats have become paramount concerns as organisations navigate uncertain futures. These leaders face a talent shortage that threatens their strategic initiatives and operational resilience.

## Talent and labour in short supply, especially for emerging technologies

The rapid pace of digital transformation is driving technology modernization, reshaping industries, and transforming business models. Disruptive innovations are redefining work, and the adoption of emerging technologies, such as AI, is creating a demand for new skill sets. This talent gap is widened by the retirement of the baby-boomer generation, leaving a void not quickly filled by new workforce entrants. Cybersecurity remains critical, with rising cyberattack frequency and sophistication. Organisations must invest in robust security measures and retain experts to defend against these threats.

*The widening talent gap and evolving skills landscape underscore the urgent need for new roles, such as AI engineers and developers.*

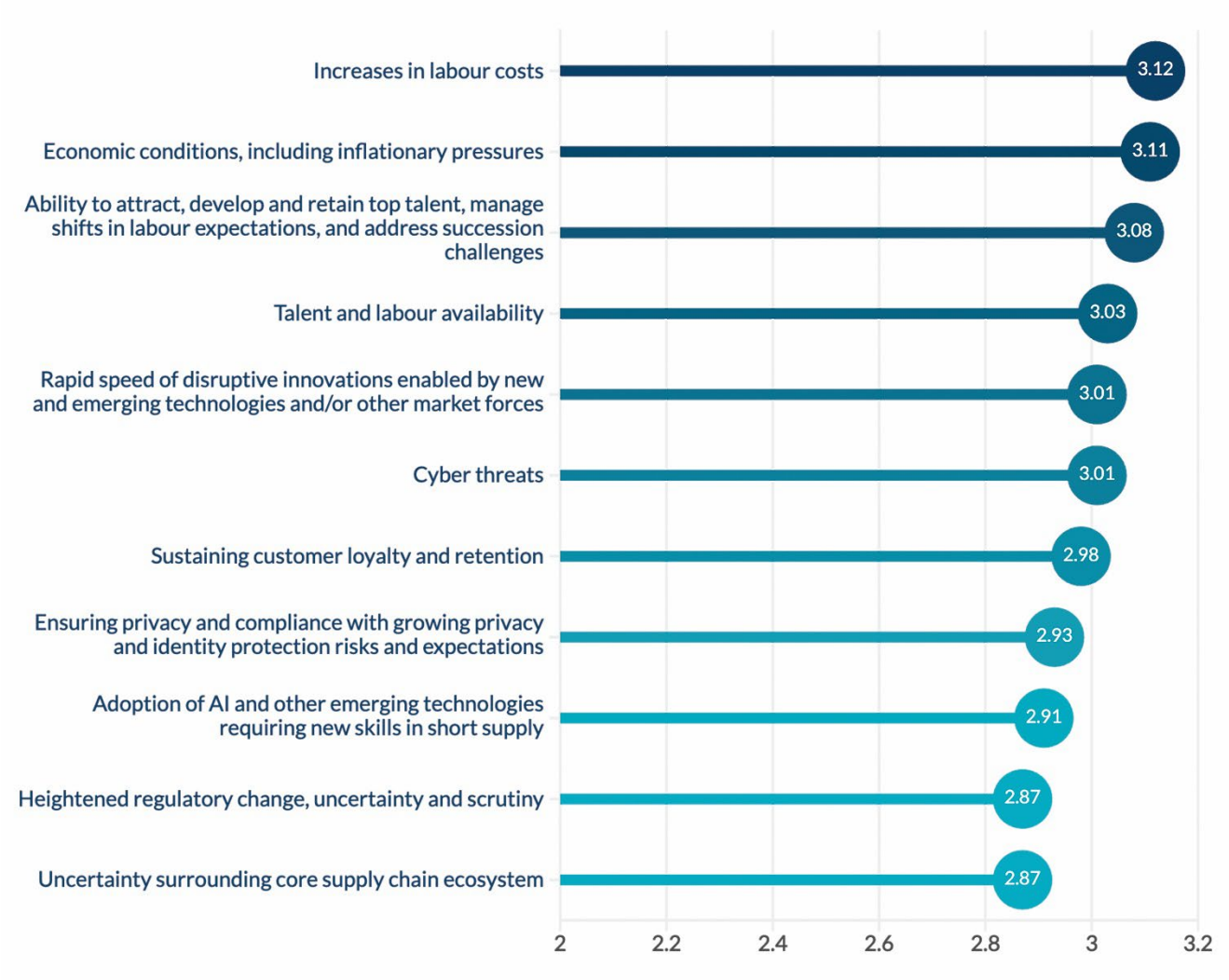
The widening talent gap and evolving skills landscape underscore the urgent need for new roles, such as AI engineers and developers, which are set to see a continuing surge in demand this year. As organisations embark on technology modernisation and innovation journeys, their technology teams are at the core of these efforts. However, finding individuals with the requisite skills to support these initiatives remains a formidable obstacle.

## Other significant themes

Other significant themes emerging from the survey include escalating concerns over economic conditions, cyber threats, and risks presented by third parties. Organisations are increasingly grappling with a complex web of national and regional laws and regulations surrounding data privacy, contingent upon their operational locales. Navigating and adhering to these myriad legal and regulatory requirements demands meticulous involvement from CIOs and CTOs.

Compounding these concerns, cyber threats continue to evolve and grow in sophistication, positioning themselves as a top-rated risk globally across most industries and executive groups. Furthermore,

organisations, including technology leaders, must vigilantly monitor economic conditions as they can shift rapidly, impacting budgets and operational models.



## A call to action for CIOs and CTOs

Considering the challenges technology leaders face concerning macroeconomic, strategic and operational risk issues, CIOs and CTOs should consider taking the following actions in their technology organisations.

## Talent and skills with the adoption of AI

**Adopt a new talent mindset.** Shift focus from hiring data scientists, systems architects, and AI specialists, to prioritizing skills over specific roles. Emphasize the value talent generates rather than its costs, and view leadership development as a shared responsibility among technology leaders. Consider variable labour models for specialized skills, utilizing consultants for project-based expertise. This approach provides access to a broader talent pool and enhances agility in meeting technological demands. Investing in continuous learning and development programmes for existing employees is essential to bridge the talent gap and prepare the workforce for emerging technologies.

**Conduct a skills inventory.** Regularly assess the technology function's skills against the organization's business strategies. Use AI-led workforce-planning and talent-intelligence tools for real-time insights into enterprise skills, evaluating their alignment with long-term objectives.

**Implement skills analytics.** Track open positions, skills at risk, and upskilling opportunities to ensure that the technology function meets strategic goals.

**Fostering a culture of innovation and collaboration is crucial.** Promoting cross-functional teams to work on AI and emerging technology projects can stimulate creativity and expedite problem-solving. Staying informed about regulatory changes and compliance requirements related to data privacy and AI ethics will help build trust with stakeholders and maintain a competitive advantage in the rapidly evolving technological landscape.

## Cyber threats

**Identify and retain cybersecurity talent.** Safeguarding against cyber threats requires the right talent. Organisations are exploring outsourcing or managed cybersecurity services to access hard-to-recruit talent and focus on in-house capabilities.

**Understand the threat of ransomware.** Companies must assess their resilience and ability to restore systems quickly, ensuring that attacks do not jeopardize partners' environments.

**Learn about the generative AI threat landscape.** Generative AI can enable sophisticated cyberattacks. Executives and boards should focus on governance and security measures, understanding how malicious actors exploit these tools and using AI to enhance attack detection and develop automated mitigation strategies.

**Evaluate cybersecurity and privacy regulations.** A risk-based approach is effective for mitigating cyber threats, but regulations on breach disclosures and privacy protections are increasing. New AI regulations

prompt organisations to evaluate control environments and implement policies to close gaps, with executives and boards advocating for compliance.

**Monitor quantum computing implications.** Quantum computing threatens existing cryptographic methods, prompting organisations to reassess data encryption strategies and pursue quantum-resistant cryptography solutions for enhanced protection against emerging threats.

## Overview of long-term risks

Looking ahead to 2035, CIOs and CTOs anticipate that many of their most pressing short-term risk concerns—talent and labour availability, adoption of AI and other emerging technologies, and cyber threats—will persist over the next decade. Technology leaders, like most executives in our study, identify talent and labour availability as the top long-term concern from a macroeconomic perspective. Meanwhile, the adoption of emerging technologies, such as AI, emerges as a top strategic risk, and cyber threats have become the foremost operational risk.

These risks, though classified and measured differently, share a common thread: They are people-centric. Each of these challenges will require talent that can adapt and master the necessary knowledge to be effective in evolving roles as technology advances.

Cyber threats will remain a significant concern as technology progresses and bad actors become more adept at hacking systems and accessing data. The growing sophistication of technologies employed by black-hat groups, nation-states, and criminal organisations is of increasing concern to CIOs and CTOs.

Though organisations are working diligently to prevent attacks and data loss, there is a prevailing perception not only that attackers will become more skilled at cybercrime but also that the tools available to them will become more powerful.

*Talent, AI adoption, and cyber threats will remain top concerns for CIOs and CTOs through 2035*

For instance, the ongoing development of AI systems will enable even the most novice cyber attackers to create highly sophisticated attacks leveraging automation and machine learning. As the potential for advanced cyber attacks becomes more alarming, CIOs and CTOs will increasingly rely on AI-powered cybersecurity operations to detect and defend against rapidly evolving threats. Furthermore, the advent of a post-quantum world, where quantum computing becomes routinely accessible, will introduce additional threats, particularly to encryption.

# Long-term risk outlook

## Macroeconomic risk issues

| Risk | Percentage |
|---|---|
| Talent and labour availability | 42% |
| Increase in labour costs | 36% |
| Economic conditions including inflationary pressures | 36% |

## Strategic risk issues

| Risk | Percentage |
|---|---|
| Adoption of AI and other emerging technologies requiring new skills in short supply | 38% |
| Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces | 34% |
| Heightened regulatory change, uncertainty and scrutiny | 26% |

## Operational risk issues

| Risk | Percentage |
|---|---|
| Cyber threats | 36% |
| Third party risks | 29% |
| Ability to attract, develop, manage shifts in labour expectations, and address succession challenges | 27% |

Note: Respondents were asked to identify the "top two" risks in each category (macroeconomic, strategic, operational) separately. That is, respondents identified six risks (two in each category) as "top two" risks. For each category, the three risk issues (including ties) receiving the most responses by percentage are shown.

## About the Executive Perspectives on Top Risks Survey

We surveyed 1,215 board members and executives across a number of industries and from around the globe, asking them to assess the impact of 32 unique risks on their organization over the next two to three years and over the next decade, into 2035. Our survey was conducted online from mid-November 2024 through mid-December 2024. For the near-term outlook, each respondent was asked to rate 32 individual risks on a five-point Likert scale, where 1 reflects "No Impact at All" and 5 reflects "Extensive Impact." For each of the 32 risks, we computed the average score reported by all respondents and rank-ordered the risks from highest to lowest impact.

We also asked executives to share their perspectives about long-term risks (over the next 10 years – 2035) by selecting the top two risks from each of the three dimensions (macroeconomic, strategic and operational). For each of the 32 risks, we calculated the percentage of respondents who included that risk as one of their two top risks for each dimension.

Read our *Executive Perspectives on Top Risks Survey* executive summary and full report at www.protiviti.com or http://erm.ncsu.edu.

## About the author

Kim Bozzella is Protiviti's Global Leader of Technology Consulting. She is responsible for the strategy, solution offerings, consulting delivery and external partnerships for all of Protiviti's technology solutions, including Security & Privacy, Enterprise Applications, Technology Strategy & Operations, Enterprise Data & Analytics, Software Services and Emerging Technologies. With over 30 years of experience in financial services industry, information technology, and consulting, Kim has been at the forefront of the convergence of technology innovation, business management, and regulatory reform.