CIOs and CTOs See Skills, Staffing and Talent as Top Risk Concerns

by Kim Bozzella
Global Leader, Technology Consulting, Protiviti

The combined analysis of risk insights from global executives for both 2024 and a decade out reveal several interrelated challenges that may result in significant events with the potential to test an organisation's business agility and resilience.

Changes in the profile of top risks from the prior year disclose a number of shifting conditions that may disrupt markets, including events triggered by intensifying geopolitical conditions. Many of those events are expected to have long-lasting impacts on business models and the competitive balance in a nuanced global marketplace.

Board members and C-suite leaders who acknowledge these changing realities and effectively tackle them with comprehensive, organisation-wide risk analyses that align with the business strategy possess unique skills. These skills position their organisation to be ready and flexible in the face of inevitable disruptive change, giving them an advantage over their competitors.

In this 12th annual survey, Protiviti and NC State University's ERM Initiative report on the top risks currently on the minds of board members and executives worldwide. The results of this global survey reflect their views on the extent to which a broad collection of risks is likely to affect their organisations over the next year – 2024 – and a decade later – 2034. Our respondent group, which includes 1,143 board members and C-suite executives from around the world, provided their perspectives about the potential impact over the next 12 months and next decade of 36 risk issues across these three dimensions:[1]

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

[1] Each respondent rated 36 individual risk issues using a 10-point scale, where a score of 1 reflects "No Impact at All" and a score of 10 reflects "Extensive Impact" to their organisation. For each of the 36 risk issues, we computed the average score reported by all respondents.

Commentary – CIOs/CTOs

Businesses today face a myriad of challenges as they work to adapt and transform their operational models in order to overcome future obstacles, including competitive pressures and cyber threats. Moreover, 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 are among numerous factors shaping the risk landscape in the eyes of CIOs and CTOs, according to the results of our latest Top Risks Survey.

Overview of top risk issues in 2024

The near-term risk concerns for CIOs and CTOs centre chiefly on people-related areas. Issues around available skills to support the adoption of digital technologies, the ability to secure talent, and succession planning are top-of-mind.

For technology leaders, attracting, developing, and retaining top talent is a significant and urgent challenge. In today's era, IT systems have a substantial impact on the ability of IT staff to address various risk concerns, such as cyber threats, adoption of digital technologies and advanced tools (like GenAI), third-party risks, and organisational resilience and agility.

CIOs, CTOs, and technology leaders know, as well as anybody, that there just isn't enough available talent and skill walking the street right now to fill their needs. Of note, the two top-ranked risk issues for CIOs and CTOs – the adoption of digital technologies requiring new skills in short supply, and the ability to attract, develop and retain top talent, manage shifts in labour expectations, and address succession challenges – have a symbiotic relationship. Both centre on access to needed talent, which continues to be in short supply and shows no sign of changing soon, particularly as the baby-boomer generation transitions into retirement without a commensurate level of people entering the workforce.

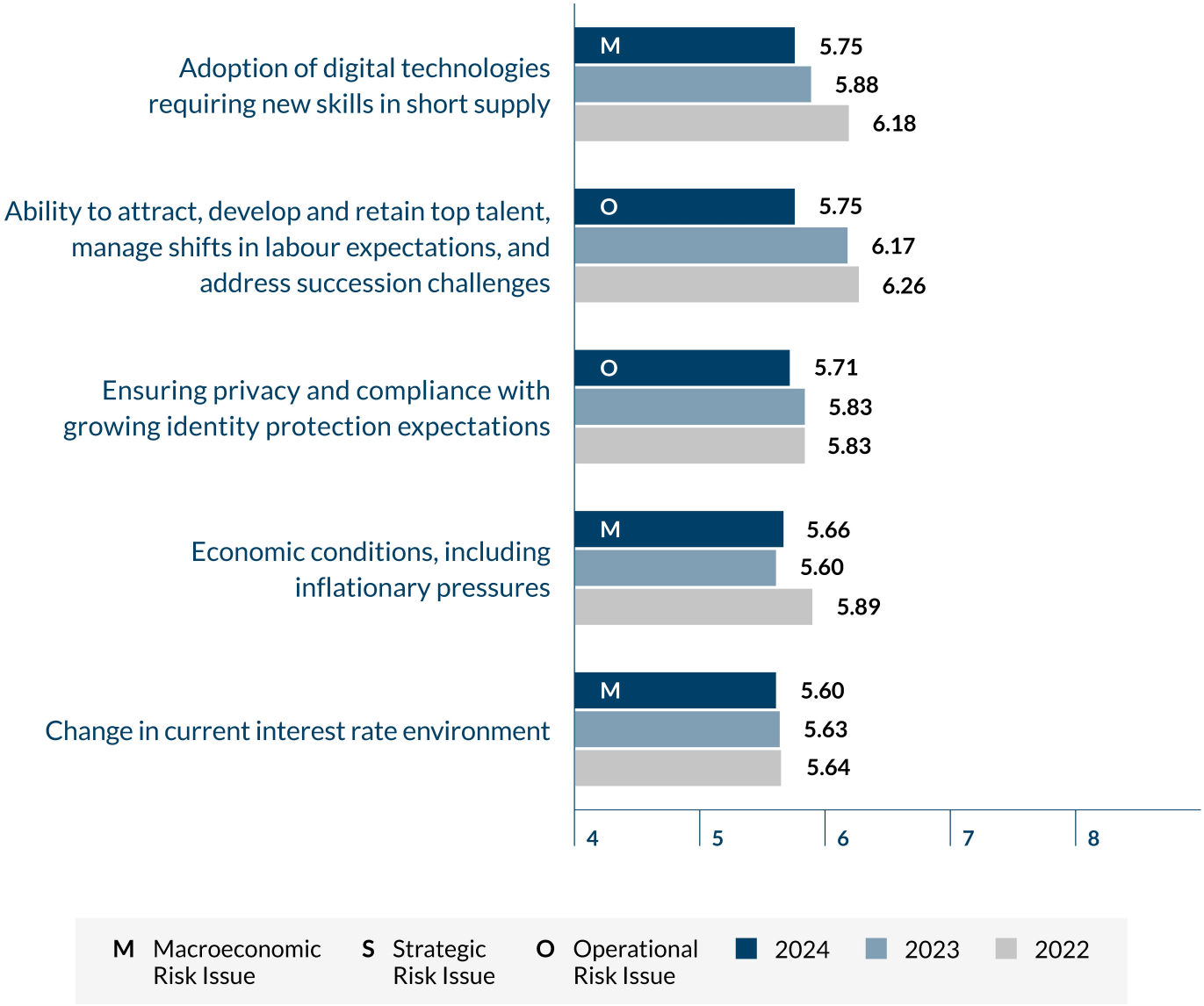
As organisations undergo transformation and innovation, their technology groups are foundational to these efforts. However, finding the right people with the right skills to support these initiatives remains a significant hurdle.

This talent gap and the changing skills landscape also highlight the need for new roles, such as AI engineers and developers, which will only grow in demand this year. As organisations undergo transformation and innovation, their technology groups are foundational to these efforts. However, finding the right people with the right skills to support these initiatives remains a significant hurdle.

Another major theme revealed in the survey is the growing concern over ensuring privacy and compliance with identity protection expectations and, by extension, cyber threats. Organisations are grappling with an increasing number of national and regional laws and regulations around data privacy, depending on where they have operations. Addressing and complying with these many laws and regulatory requirements necessitates detailed involvement by CIOs and CTOs. Adding to these concerns, cyber threats continue to evolve and become more sophisticated, making them a top-rated risk globally for most industries and executive groups. While not rated as high by CIOs and CTOs specifically, cyber risks likely are reflected in their concerns about identity protection.

Economic conditions and changes in the interest rate environment are also significant sources of concern. Continued uncertainty in the economy, along with persistent inflationary trends and higher interest rates globally (albeit with recent signs of easing), has increased the cost of doing business. Organisations, including technology leaders, need to monitor economic conditions closely as they can shift rapidly and affect their budgets and operating models.

Top five risks for CIOs/CTOs – 2024



Overview of top risk issues in 2034

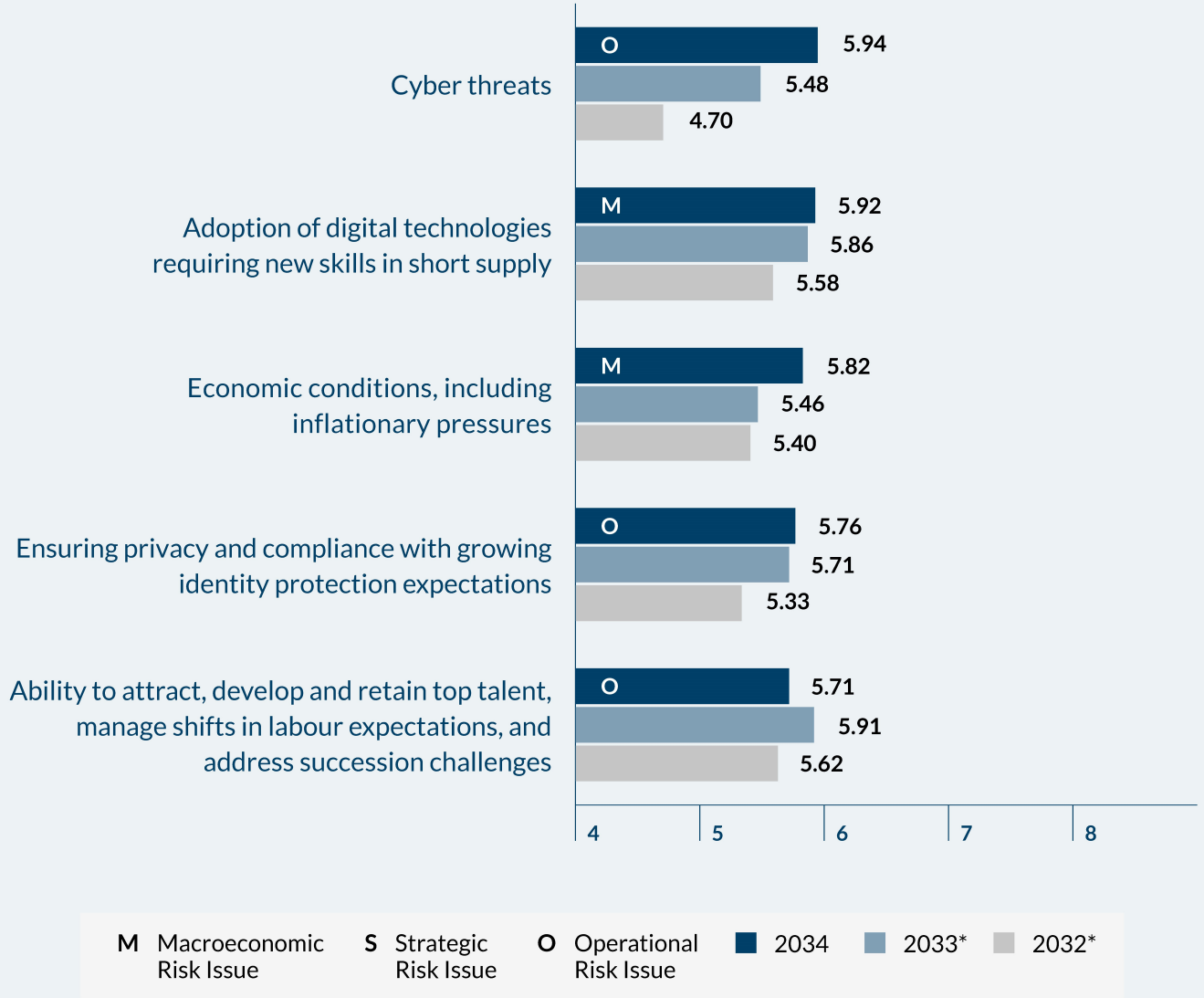
Looking ahead to 2034, CIOs and CTOs see many of their most pressing short-term risk concerns (adoption of digital technologies, talent challenges, economic conditions) persisting over the next decade.

Technology leaders, like most executives in our study, see cyber threats as the top long-term concern for organisations, especially as technology advances and bad actors become more adept at hacking systems and

accessing data. The growing sophistication of technologies that Black-Hat groups, nation-states and criminal organisations are using to attack systems and data are of increasing concern to CIOs and CTOs. In an unfortunate reality, it's likely that many executives view a cyber breach in their organisations as inevitable sometime within the next 10 years.

While organisations are working hard to prevent attacks and data loss, there is a perception that attackers will not only become more adept at cybercrime, but also that the tools available to them will become more accessible and advanced. Consider, for example, the ongoing development of quantum computing. Once we enter a post-quantum world, where quantum computing is routinely accessible, there will be additional threats, particularly to encryption. If we combine this with the increasing use of automation and speed at which AI is being developed and deployed in organisations, the potential for sophisticated cyber attacks becomes even more concerning.

Top five risks for CIOs/CTOs – 2034



* This data was reported as 2032 and 2031 results, respectively, in our prior year reports. We have shifted our terminology to reflect a decade out, thus have revised these year references in the interests of clarity.

A call to action for CIOs and CTOs

Considering the challenges technology leaders face concerning the accessibility of talent and requisite skills, along with cyber and privacy threats, CIOs and CTOs should consider taking the following actions in their technology organisations:

Talent and skills

Adopt a new talent mindset. Your organisation cannot rely on the ability to "go hire more" data scientists, systems architects, AI specialists, or other in-demand talent whenever it wants. Such types of prized skills are not widely available. Focus on skills instead of roles or jobs, prioritise the value talent generates over its costs, and treat leadership development and succession planning as a shared responsibility among all leaders on the technology team. Evaluate opportunities to employ variable labour models for specialised and/or high-demand skills.

Take a talent inventory. Perform regular assessments of the technology function's talent and skills. Map these to the skills and talent required to achieve the organisation's short- and long-term business strategies. AI-driven workforce planning/design software and talent intelligence tools can produce detailed, real-time views of all the skills that reside throughout the enterprise. Evaluate these talent inventories based on their alignment with longer-term business objectives.

Deploy new skills analytics. Measure and report on open positions, skills at risk and upskilling opportunities. These metrics help monitor organisational effectiveness, which is the extent to which the technology function is delivering on strategic objectives.

Cyber threats

Understand the substantial threat of ransomware. As companies focus on defending and protecting themselves against ransomware attacks, they also need to understand their resiliency and ability to restore systems to not only become operational on a timely basis but also to demonstrate that any attack would not be a threat to their partners' environments. Partners sharing their network connections and data need to be convinced that malicious payloads wiped from the company's environment are not a threat to theirs (and vice versa).

Identify and retain cybersecurity talent. As more businesses implement emerging technologies, the need to protect against cyber threats and have the right talent in place to set and execute the cybersecurity framework becomes increasingly important. This reality requires businesses to think about their cybersecurity talent strategy. To that end, many organisations are considering outsourcing or leveraging cybersecurity managed services from other organisations to buy the talent that they may not be able to hire on their own. This approach allows them to focus on defining the capabilities they need in-house.

Learn the generative AI threat landscape. Generative AI can fuel more sophisticated attacks. Executives and boards are paying attention to this area through different angles. One is establishing appropriate governance and security around generative AI tools that are being created and used to drive the business strategy. The other is understanding how bad actors are using these tools to create complex attacks on organisations and leveraging vulnerabilities at an alarming pace to outsmart defences. Consider how to leverage generative AI to aid in identifying attacks and establishing more effective automated mitigation capabilities.

Assess proliferating cybersecurity and privacy regulations. While a risk-based approach is best practice in addressing cyber threats, there is an increasing focus on additional regulations requiring cybersecurity breach disclosures and various privacy regulations intended to protect consumers and individuals. Additional regulations related to AI are driving organisations to map their existing control environment against these evolving requirements and establish new policies and controls to address any gaps that may exist. Expect executives and boards to push their organisations to establish defensible positions related to these regulations.

Keep an eye on quantum computing's impact on cyber. The rise of quantum computing has the ability to render obsolete existing cryptography methods. This is an area where organisations are starting to evaluate their strategy around encrypting data and establishing innovations to deploy quantum-resistant cryptography to secure against attacks that are backed by quantum computing's increased computing power.

About the Executive Perspectives on Top Risks Survey

We surveyed 1,143 board members and executives across a number of industries and from around the globe, asking them to assess the impact of 36 unique risks on their organisation over the next 12 months and over the next decade. Our survey was conducted in September and October 2023. Respondents rated the impact of each risk on their organisation using a 10-point scale, where 1 reflects "No Impact at All" and 10 reflects "Extensive Impact." For each of the 36 risks, we computed the average score reported by all respondents and rank-ordered the risks from highest to lowest impact.

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

Contact

Kim Bozzella
Managing Director
Global Leader, Technology Consulting
kim.bozzella@protiviti.com