protiviti®
Global Business Consulting

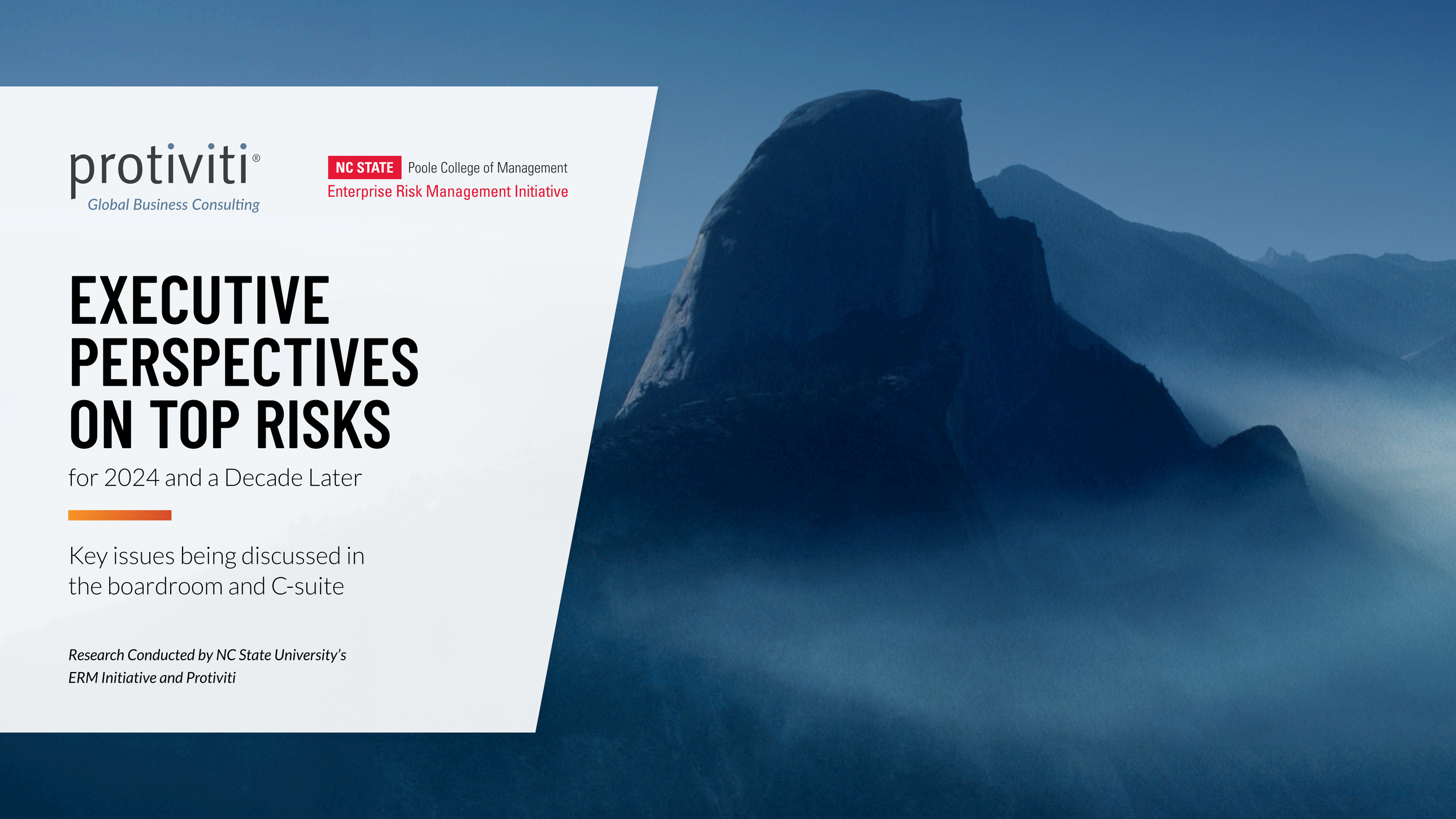
NC STATE Poole College of Management
Enterprise Risk Management Initiative

EXECUTIVE PERSPECTIVES ON TOP RISKS

for 2024 and a Decade Later

Key issues being discussed in the boardroom and C-suite

Research Conducted by NC State University's ERM Initiative and Protiviti



Contents

Protiviti and NC State University's ERM Initiative are pleased to provide our 12th annual report focusing on the top risks currently on the minds of 1,143 directors and senior executives around the globe. This report reflects 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.

The top 10 risk lists for the next 12 months (2024) and 10 years out (2034)

The table to the right summarises the top 10 risks for 2024 and 2034. As indicated by the red arrows, three of the top 10 risks for 2024 are rated higher than they were for 2023, and nine of the 2034 risks are higher than last year's survey that also looked out a decade. Eight of the top 10 risks for 2024 as well as eight top risks looking out a decade (2034) were also long-term risks in last year's survey, suggesting these risks may have a persistent long-term impact.

Top risks for 2024	
1. Economic conditions, including inflationary pressures	↓
2. Ability to attract, develop and retain top talent, manage shifts in labour expectations, and address succession challenges	↓
3. Cyber threats	↑
4. Third-party risks	↑
5. Heightened regulatory changes and scrutiny	↑
6. Adoption of digital technologies requiring new skills in short supply	↓
7. Existing operations and legacy IT infrastructure unable to meet performance expectations as well as "born digital" competitors	↓
8. Change in current interest rate environment	↓
9. Increases in labour costs	↓
10. Ensuring privacy and compliance with growing identity protection expectations	↓

Top risks for 2034	
1. Cyber threats	↑
2. Ability to attract, develop and retain top talent, manage shifts in labour expectations, and address succession challenges	↑
3. Adoption of digital technologies requiring new skills in short supply	↑
4. Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces	↑
5. Heightened regulatory changes and scrutiny	↑
6. Third-party risks	↑
7. Economic conditions, including inflationary pressures	↑
8. Existing operations and legacy IT infrastructure unable to meet performance expectations as well as "born digital" competitors	↑
9. Increases in labour costs	↑
10. Inability to utilise rigorous data analytics to achieve market intelligence and increase productivity and efficiency	↓

Key highlights from this study

Major themes for 2024 and 2034

- **Multiple sources of uncertainty create potential for a wide range of near-term horizon risks.** The shift in top risks from last year reveals a global business environment experiencing significant change, with many new risk concerns for 2024 relative to last year.
- **Recent geopolitical developments are changing the risk landscape.** Prior to the October 7, 2023, developments in the Middle East, no risks were rated at the "Significant Impact" level for 2024; however, after the attacks, many risks increased, with four rated at the "Significant Impact" level.
- **Economic concerns zoom to the top risk position near-term.** Economic conditions, particularly inflationary pressures, replaced the ability to attract, develop and retain top talent, manage shifts in labour expectations, and address succession challenges as the number one risk globally for 2024.
- **Myriad technology-related challenges include escalated cybersecurity risks, continued data privacy concerns linked to increased third-party reliance, the need to upskill employees to realise fully the value proposition of emerging technologies, and the limitations of legacy infrastructure.** These technology-linked risks are interrelated and need to be considered collectively by executives and the board, as exposures triggered by one risk may lead to increased exposure to other risks.
  - **Cybersecurity represents an ongoing challenge for both the near-term and long-term.** Challenges related to cyber threats are increasingly on the minds of global executives, moving from the 15th-ranked risk last year to the third-ranked risk for 2024 and the top risk for 2034, up from 15th in last year's long-term horizon assessment. The increasing use of technology to drive innovation and efficiencies and increased reliance on third parties create more opportunities for cyber vulnerabilities to be exposed, particularly to nation-state and other threat actors determined to exploit these opportunities for geopolitical advantages and financial gain.
  - **Legacy IT systems and existing operations may make it difficult for incumbents to compete with nimbler "born digital" competitors.** Not only do outdated systems create competitive limitations, but they also present unintended exposures that may lead to cybersecurity and data privacy concerns. Executives reveal this as both a short-term and long-term top 10 risk concern.
  - **Coupled with cyber threat concerns, executives are also focused on the challenge of addressing proliferating identity protection expectations.** As regulations proliferate and overall public expectations surrounding the protection of sensitive, private data evolve, business leaders are concerned about their organisation's ability to protect the information they collect, process, store and manage from unintentional exposure.
- **People-related risks intertwine the top near-term and long-term risks.** Talent-related issues dominated the top risks in the prior year's survey, and executives continue to focus on risks related to finding and retaining the right kind of talent for their organisation's strategic success. Overarching concerns about attracting, developing and retaining top talent, including succession challenges, remain near the top of all risk issues (as the number two risk for 2024), with that concern continuing for the long term (it remains as the number two risk for 2034). Relatedly, executives are particularly focused on challenges associated with attracting unique kinds

of talent and upskilling existing employees, which will allow their organisations to embrace emerging digital technologies, with that particular concern making the top 10 list of risks for both 2024 and 2034. Given this race for talent, executives continue to note that increases in labour costs will be a challenge now and a decade later.

- **Third-party risks rise in importance.** Challenges related to existing core operations and legacy IT systems, competitive pressures, pursuits to achieve greater efficiencies, and difficulties in attracting talent may be motivating organisations to increase the use of joint ventures, alliances and various kinds of third-party relationships to manage a number of processes. With greater reliance on third parties to perform critical business services, executives are increasingly focused on new risks that may emerge in light of these external partnerships. Among all 36 risks considered by executives in this year's survey, risks linked to third parties increased the most from the prior year, moving from the 17th position last year to the 4th position for 2024. It also made the top 10 list of risks for a decade out.

- **Regulatory changes and scrutiny are heightened for the near-term and a decade out.** The potential for expansion in rules and regulatory oversight is creating increased concerns not only for 2024, but also 2034 given it represents a top five risk for both the near-term and long-term horizons. Specific regulatory risks vary by industry. For example, recently proposed laws and regulations in financial services may increase capital and liquidity requirements and compliance costs, resulting in reduced returns. Technology companies face increasing regulatory oversight on a number of fronts. Such concerns are pervasive across other industries, as worries about expanding government regulations and agency enforcement — particularly related to data privacy, climate disclosures, sustainability reporting, cyber breach disclosures, expanded attestation requirements and other matters — are higher than reported in last year's survey for both the coming year and a decade out.

- **Looking out a decade highlights how many short-term risks are likely to have a lingering impact over the next 10 years.** Eight of the top 10 risks for 2024 are top 10 risk concerns in 2034, although there are shifts in relative importance within the top 10. This signals the importance of thinking robustly about responses to these risks, given their relative importance for both short-term and long-term performance. Furthermore, eight of the top 10 risks looking out 10 years in last year's survey remain on the top 10 list for 2034.

  Interestingly, respondents signal a heightened overall risk concern as they look out a decade, given they rated nine of the top 10 risks higher for 2034 than they did when looking out a decade in last year's survey. The persistence of these risks, continued occurrence of unexpected events and the spectre of intensifying geopolitical tensions create a nuanced view of the future. On the geopolitical front, for example, Russia's aggression in Ukraine, the war in the Middle East, the declining trust in American institutions, the proliferation of disinformation and propaganda, and the convergence of China, Russia, Iran and North Korea in opposition to Western democracies provide a combustible mix that is likely impacting leaders' assessment of the long-term global risk landscape.

- **Disruptive innovations and the inability to utilise rigorous data analytics are creating significant pause for executives as they think about their organisation's long-term competitive positioning.** Continued advances in artificial intelligence (AI) and other technologies are driving a wave of disruption that will impact business models, sweep away obsolete strategies and alter customer experiences. Navigating the rapid pace of these digital innovations and finding ways to leverage insights from the volumes of data organisations must evaluate are particularly concerning to executives as they think about their organisations a decade from now. Those technology and innovation concerns cannot be separated from other risk concerns making the top 10 for 2034 related to shortages of talent to manage the adoption of digital technologies, the dependence on legacy IT systems, and overarching cyber and privacy concerns. Once again, these interconnected risks cannot be viewed in isolation.

The interrelated nature of the risks comprising the top 10 for both the near-term and a decade later highlight the importance of managing risks from a portfolio, enterprisewide perspective. Evaluating risks individually may overlook the reality that a single risk event may be sourced across multiple risk concerns. Robust conversations about assumptions related to the organisation's future, overlapping root causes across different risks and dependences on single responses to manage multiple risks can benefit executives and boards with insights about how a given risk may interact with others to impact an organisation's strategic success and long-term viability.

Methodology

We are pleased with the global reach of our 12th annual survey, with strong participation from 1,143 respondents across a variety of industries. Our survey captures insights from C-suite executives and directors, 43% of whom represent companies based in North America, 16% in Europe, 11% in Asia, 9% in Latin America, and 8% in Australia/New Zealand, with the remaining 13% from India, Africa and the Middle East.

Our survey was conducted online in September and October of 2023 to capture perspectives on risks on the minds of executives as they peered into 2024 and a decade later (2034). Each respondent was asked to rate 36 individual risk issues across three dimensions.

- **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

Table 1 lists the 36 risk issues rated by our respondents. Each risk was rated in terms of its relative impact 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 over the next year. We also asked them to consider how each of these risks was likely to affect their organisation 10 years in the future (i.e., in 2034).

For each of the 36 risk issues, we computed the average score reported by all respondents. Using mean scores across respondents, we rank-ordered risks from highest to lowest impact. This approach enabled us to compare mean scores across the past three years to highlight changes in the perceived level of risk.

Consistent with our prior studies, we grouped all the risks based on their average scores into one of three classifications:

- Risks with an average score of **6.0 or higher** are classified as having a **"Significant Impact"** over the next 12 months (2024)/over the next decade (2034).
- Risks with an average score of **4.51 through 5.99** are classified as having a **"Potential Impact"** over the next 12 months (2024)/over the next decade (2034).
- Risks with an average score of **4.50 or lower** are classified as having a **"Less Significant Impact"** over the next 12 months (2024)/over the next decade (2034).

We refer to these risk classifications throughout our report as we provide high-level insights from taking a portfolio view of both the short-term and long-term risk issues. We follow that with detailed sub-analyses across a variety of dimensions.

We begin with an overview of overarching risk insights based on a collective analysis of both short-term and long-term risk findings from our survey. Following that overview, we highlight several calls for action that executives may want to consider as they evaluate the effectiveness of their organisation's risk governance processes in light of the key findings.

In addition to the global, overarching insights, we also review results for various subgroups (i.e., company size, position held by respondent, industry representation, geographic location and organisation type). With respect to the various industries, we grouped related industry sectors into combined industry groupings to facilitate analysis, consistent with our prior years' reports.

We conclude this report with a discussion of plans among organisations to improve their capabilities for managing risks and end with diagnostic questions executives and directors may find helpful to consider when evaluating risk assessment and risk management processes.

TABLE 1

List of 36 risk issues analysed

Macroeconomic Risk Issues

- **Increases in labour costs —** Anticipated increases in labour costs may affect our opportunity to meet profitability targets
- **Volatility in global financial markets and currency exchange rates —** Anticipated volatility in global financial markets and currency exchange rates may create significantly challenging issues for our organisation to address
- **Changes in global markets and trade policies —** Evolving changes in assumptions underlying globalisation and in global trade policies, escalating tariffs, border restrictions, targeted embargoes, shifts to multilateralism and emergence of regional trading alliances may affect our ability to operate and source effectively and efficiently in international markets
- **Access to capital/liquidity —** Our ability to access sufficient capital/liquidity may restrict growth opportunities for our organisation
- **Economic conditions, including inflationary pressures —** Economic conditions (including inflationary pressures) in markets we currently serve may significantly restrict growth opportunities, impact margins or require new skill sets for our organisation
- **Adoption of digital technologies requiring new skills in short supply —** The adoption of digital technologies (e.g., artificial intelligence, automation in all of its forms, natural language processing, visual recognition software, augmented/virtual reality simulations and the metaverse) in the marketplace and in our organisation may require cross-functional skills in Agile, Lean and design that are in short supply in the market as well as significant efforts to upskill and reskill existing employees to fully utilise the new capabilities
- **Geopolitical shifts, regional conflicts and instability in governmental regimes or expansion of global terrorism —** Political uncertainty surrounding the influence and continued tenure of key global leaders, geopolitical shifts, regional conflicts, and instability in governmental regimes or expansion of global terrorism may restrict the achievement of our global growth and profitability objectives
- **Change in current interest rate environment —** The current interest rate environment may have a significant effect on the organisation's capital costs and operations
- **Pandemic-related government policies and regulation —** Government policies surrounding public health practices (in response to a pandemic) and stimulus to drive recovery and national resilience may significantly impact the performance of our business
- **Impact of social issues and DEI priorities on ability to attract/retain talent and compete —** Shifts in perspectives and expectations about social issues and priorities surrounding diversity, equity and inclusion (e.g., board composition, representation in the C-suite and leadership ranks, and onboarding policies) are occurring faster than the pace at which our organisation is motivated and able to manage effectively, which may significantly impact our ability to attract/retain talent and compete in the marketplace

Strategic Risk Issues

- **Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces —** Rapid speed of disruptive innovations enabled by advanced technologies (e.g., artificial intelligence, including advancements such as generative AI; automation in all of its forms; hyper-scalable platforms; faster data transmission; quantum computing; blockchain; digital currencies; and the metaverse) and/or other market forces may outpace our organisation's ability to compete and/or operate successfully without making significant changes to our business model
- **Social media developments and platform technology innovations —** Rapidly expanding developments in social media, including the spread of misinformation and disinformation, and platform technology innovations may significantly impact how we do business, interact with our customers, ensure regulatory compliance and/or manage our brand
- **Heightened regulatory changes and scrutiny —** Regulatory changes and scrutiny may heighten, noticeably affecting the way our processes are designed and our products or services are produced or delivered
- **Growing focus on climate change and other sustainability policies, regulations, and expanding disclosure requirements as well as expectations of key stakeholders —** Growing focus on climate change and other sustainability issues and related ESG policies, regulations and expanding disclosure requirements, as well as expectations and emerging regulations of governments, current and potential employees, and other stakeholders about "green" initiatives, supply chain transparency, fairness in reward systems, and other governance and sustainability issues, may require us to significantly alter our strategy and business model in ways that may be difficult for us to implement as timely as the actions of our competitors
- **Ease of entrance of new competitors or other changes in competitive environment —** Ease of entrance of new competitors into the industry and marketplace or other significant changes in the competitive environment (such as major market concentrations due to M&A activity) may threaten our market share
- **Organisation not sufficiently resilient and/or agile to manage an unexpected crisis —** Our organisation may not be sufficiently resilient and/or agile to manage an unexpected crisis (including a catastrophic event) significantly impacting our operations or reputation
- **Difficulty in growing through acquisitions, joint ventures and other activities —** Growth opportunities through acquisitions, joint ventures and other partnership activities may be difficult to identify and implement
- **Limited opportunities for organic growth —** Opportunities for organic growth through customer acquisition and/or enhancement may be significantly limited for our organisation
- **Substitute products and services that affect the viability of our business —** Substitute products and services may arise from competitors that enhance the customer experience and affect the viability of our current business model and planned strategic initiatives
- **Sustaining customer loyalty and retention —** Sustaining customer loyalty and retention may be increasingly difficult due to evolving customer preferences for different products, services and buying experiences and/or demographic shifts in our existing customer base
- **Performance shortfalls that trigger activist shareholders —** Performance shortfalls (including lack of progress on ESG goals/expectations) may trigger activist shareholders who seek significant changes to our organisation's strategic plan and vision
- **Formulating business response to legal, political and social issues that are polarising —** Our organisation may not be prepared to formulate and communicate effectively its response to legal, political and social issues and other related market developments that are polarising to key stakeholders*

* This risk is new to the 2024 survey.

Operational Risk Issues

- **Challenges in sustaining culture due to changes in overall work environment —** Changes in the overall work environment, including shifts to hybrid environments, expansion of digital labour (e.g., through the impact of generative AI), changes in the nature of work and who does that work, and M&A activities, may lead to challenges to sustaining our organisation's culture and business model***
- **Uncertainty surrounding core supply chain ecosystem —** Uncertainty surrounding our organisation's core supply chain including the viability of key suppliers, scarcity of supplies, reshoring/offshoring/friend-shoring initiatives, energy sources, unpredictable shipping and distribution logistical issues, or lack of price stability in the supply chain ecosystem may make it difficult to deliver our products or services at acceptable margins
- **Third-party risks —** Third-party risks arising from our reliance on outsourcing and strategic sourcing arrangements, ecosystem partners, IT vendor contracts, and other partnerships/joint ventures to achieve operational and go-to-market objectives may prevent us from meeting organisational targets or impact our brand image
- **Ability to attract, develop and retain top talent, manage shifts in labour expectations, and address succession challenges —** Our organisation's ability to attract, develop and retain top talent, navigate evolving labour expectations and demands (including generational distinctions), and address succession challenges amid the constraints of a tightening talent/labour market may limit our ability to achieve operational targets
- **Cyber threats —** Our organisation may not be sufficiently prepared to manage cyber threats such as ransomware and other attacks that have the potential to significantly disrupt core operations and/or damage our brand
- **Enhanced exposure to fraud in the industry —** Incidents of fraud are increasing in our industry, which may lead to increased costs and damage to our reputation*
- **Ensuring privacy and compliance with growing identity protection expectations —** Ensuring data privacy and compliance with growing identity protection expectations and regulations may require alterations demanding significant resources to restructure how we collect, store, share and use data to run our business
- **Existing operations and legacy IT infrastructure unable to meet performance expectations as well as "born digital" competitors —** Our existing operating processes, in-house talent, legacy IT infrastructure, lack of digital expertise and/or insufficient digital knowledge and proficiency in the C-suite and boardroom may result in failure to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, including those that are either "born digital" or investing heavily to leverage technology for competitive advantage
- **Inability to utilise rigorous data analytics to achieve market intelligence and increase productivity and efficiency —** Inability to utilise advanced data analytics and "big data" to achieve market intelligence, gain insights on the customer experience, and increase productivity and efficiency may significantly affect our management of core operations and strategic plans
- **Resistance to change restricting organisation from adjusting business model and core operations —** Resistance to change in our culture may restrict our organisation from making necessary adjustments to the business model and core operations on a timely basis

* This risk is new to the 2024 survey.
** This risk was new to the 2023 survey.
*** This risk was new to the 2022 survey.

Operational Risk Issues (continued)

- **Organisation's culture not sufficiently encouraging timely identification and escalation of emerging risk issues —** Our organisation's culture may not sufficiently encourage the timely identification and escalation of emerging risk issues and market opportunities that have the potential to significantly affect our core operations and achievement of strategic objectives
- **Meeting expectations around protecting health and safety of employees (including their well-being and mental health), customers, suppliers and our communities —** Our ability to meet expectations around protecting the health and safety of employees (including their well-being and mental health), customers, suppliers and the communities in which we operate may be insufficient to receive market permission to operate or encourage people to work for us or do business with us and to do so in a safe environment
- **Managing demands on or expectations of workforce to work remotely or as part of a hybrid work environment —** Our approach to managing ongoing demands on or expectations of a significant portion of our workforce to "work remotely" or increased expectations for a transformed, collaborative hybrid work environment and distributed workforce may negatively impact our ability to retain talent as well as the effectiveness and efficiency of how we operate our business
- **Rising threat of catastrophic natural disasters and weather phenomena —** The rising threat associated with catastrophic natural disasters and weather phenomena (e.g., wildfires, floods, extreme heat/cold, cyclones/hurricanes/typhoons) may create significant operational challenges that threaten our assets and employees as well as our ability to deliver products and services to customers**

* This risk is new to the 2024 survey.
** This risk was new to the 2023 survey.

Major takeaways about emerging risks

What you need to know

The big picture: The churn in this year's survey results points to multiple sources of uncertainty, painting a cloudy, interconnected picture of the business landscape.

- Near term, there is continued economic uncertainty causing executives to sharpen their focus on managing external risks (inflation, cyber threats, interest rates, third-party exposures, etc.) and increasing organisational resilience. Long term, executives remain on guard for what comes next — as illustrated by the uptick in risks following recent events in the Middle East.

A key point: Geopolitical events are driving notable changes in global risk perceptions.

- Cyber threats, third-party risks, economic conditions, and the ability to attract and retain talent are among many other risk issues exhibiting a significant ratings jump post October 7 in our survey. Clearly, events in the Middle East are elevating long-term concerns.

Economic conditions, including inflation, represent the top risk issue for 2024.

- Uncertainty continues in the market over central bank policies amid persistent inflation being fuelled by rising labour costs (driven by skilled labour shortages), outsized government stimulus, the West's de-risking reliance upon China, regional conflicts, and other developments in the geopolitical landscape.
- Underlying the uneasiness about the economy are concerns around the current interest rate environment significantly affecting the organisation's capital costs and operations.

Cybersecurity is the most pressing risk issue when combining near- and long-term views.

- Elevated cybersecurity concerns reflect growing recognition of a complex cyber risk landscape that is impacted by the exponential curve of technological advances, increasing reliance on third parties and other market forces.
- Ensuring compliance with growing identity protection expectations made the top 10 for 2024 as well, demonstrating the interrelated nature of cybersecurity and privacy risks.

Data privacy and "big data" remain key areas of focus.

- Organisations successful in deploying forward-looking lead indicators and integrated analytics are likely to be more anticipatory and less reactive than those that aren't.

People-related risks also remain top of mind.

- Finding and keeping talent remains a major concern, even amid an uneven economy searching for a soft landing.
- Initiatives to embrace new technologies necessitate the need to reskill and upskill employees, presenting a challenge both now and in the future; so do rising labour costs.

Third-party risks rise in importance.

- This is likely due to increasing reliance on outsourcing and strategic sourcing arrangements, ecosystem partners, IT vendor contracts, and other partnerships and joint ventures to achieve operational and go-to-market objectives. Cyber threats and regulatory compliance risks also come into play.

Regulatory changes and scrutiny loom both near- and long-term.

- As continued economic uncertainty increases the likelihood governments and various agencies will interfere with market functions through regulatory overreach and even excess, there is uncertainty over the likelihood and magnitude of industry-specific and pervasive changes in the regulatory landscape.

Climate change and sustainability risks have elevated and are rated as a top five risk by respondents from Europe and the Middle East.

The combined analysis of risk insights from global executives for both 2024 and a decade out reveals 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 recognise these shifting realities and address them through robust, enterprisewide risk analyses that are aligned with business strategy possess a differentiating skill that positions their organisation's readiness and ability to adjust and pivot in the face of inevitable disruptive change as well as or better than their competitors.

There are a number of significant takeaways from this year's study for boards and executives to consider:

The churn in this year's survey for 2024 and escalation of importance of several risks point to multiple sources of uncertainty, painting a cloudy picture of the business landscape.

While not a surprise, our research results confirm that organisational risk profiles are sensitive to events and risks that can emerge rapidly and sometimes unexpectedly. The escalation of the importance of multiple near- and long-term risks conveys the stark reality of disruptive change in today's dynamic times. In the near term, there is continued economic uncertainty causing executives to sharpen their focus on managing external risks (inflation, cyber threats, interest rates, third-party exposures, etc.) and increasing organisational resilience. As for the longer term, executives remain on guard for what comes next — as illustrated by recent events in the Middle East.

Geopolitical events drive notable changes in risk perceptions.

A notable trend in our global results this year is what the findings reveal before and after October 7, 2023, when events in Israel and Gaza erupted. Based on the responses submitted prior to this date, no risks were rated at the "Significant Impact" level for 2024, whereas after this date four risks are rated at this level: economic conditions (including inflationary pressures), cyber threats, ability to attract and retain talent, and third-party risks. In addition, the scores for most risk issues increased post October 7, including the risk related to geopolitical shifts, regional conflicts and instability in governmental regimes or expansion of global terrorism.

What's even more telling are the risk scores in the 10-year outlook. Whereas five of the long-term risk issues were rated at the "Significant Impact" level among responses submitted prior to October 7, respondents after this date rated 12 at this level. Among the many notable jumps in scores, the geopolitical-related risk issue rose from 5.35 prior to October 7 to 6.06 after this date — highlighting it as "Significant Impact." Cyber threats, third-party risks, economic conditions, and the ability to attract and retain talent are among many other risk issues exhibiting a significant ratings jump. Clearly, events in the Middle East are elevating long-term concerns among directors and C-suite leaders about the impact on their businesses.

Economic conditions, including inflation, represent the top risk issue for 2024.

Economic conditions, including inflationary pressures, are the top-rated risk overall for 2024 (up from second in 2023). Near term, uncertainty continues in the market over central bank policies amid persistent inflation being fuelled by rising labour costs (driven by robust employment and skilled labour shortages, particularly in countries where birth rates have dropped significantly), outsized government stimulus, the West's de-risking reliance upon China, regional conflicts, other developments in the geopolitical landscape, and increasing shelter, food and energy prices. The open question is whether these market developments and policies will lead

to some form of soft landing or to either a mild or severe recession; or worse, a sustained period of stagnant growth. Organisations may face a dramatic change in the business landscape in the coming year, especially considering recent events in the Middle East and their potential to spread throughout the region.

Underlying the uneasiness about the economy are concerns around the current interest rate environment significantly affecting the organisation's capital costs and operations. Of note, while the rating for most risks in our survey decreased year-over-year looking out 12 months, economic risk declined the least among those risks that decreased from last year's survey, remaining relatively stable year-over-year. Looking out 10 years, economic conditions represent the seventh-ranked risk. Economic headwinds remain a concern over the long-term, beyond the shorter-term issues such as inflationary trends that are driving current concerns.

Cybersecurity is the most pressing risk issue when combining near- and long-term views.

While the economy is the top-ranked risk for the coming year, cyber threats arguably stand out as the most significant risk issue for boards and C-suite leaders when assessing both near- and long-term outlooks. For the next decade, cyber threats jumped from the 13th-ranked risk in last year's study to the top-rated risk for the 2034 outlook. For this time period, the risk rating for cyber threats increased more than 11% — by far the largest risk rating increase noted in the survey. Cyber concerns are also elevated near term, jumping from 15th in last year's survey to third this year when looking out 12 months.

Elevated cybersecurity concerns reflect growing recognition of a complex cyber risk landscape that is impacted by the exponential curve of technological advances. Specifically, considering the significance with which boards and C-suite leaders view this risk over the next 10 years, it's possible that technologies such as AI (including generative AI), cloud, and even the anticipated emergence of quantum computing and how organisations will secure their data and operations in a post-quantum world are raising significant security-related questions and concerns in the boardroom and C-suite. But other forces, such as increasing reliance on third parties and geopolitical tensions, also contribute to the threat landscape. Regarding the geopolitical picture, competing national interests, nation-state territorial aspirations and global terrorism are powerful forces that can affect cyber risk assessments in particular regions and countries.

Ensuring privacy and compliance with growing identity protection expectations made the top 10 for 2024 as well, demonstrating the interrelated nature of cybersecurity and privacy risks.

Amid economic and cyber concerns, people-related risks also remain top of mind; culture and workplace evolution have taken a back seat — at least for now.

A number of important themes related to people and culture emerged from our results:

- **Finding and keeping talent remains a major concern, even amid an uneven economy.** This is the second highest-ranked risk for both 2024 and 2034.
- **The need to reskill and upskill employees is a challenge both now and in the future.** The state of labour markets and the expected adoption of digital technologies requiring new skills in short supply are such that significant efforts will be necessary to upskill and reskill existing employees over the next decade. This is the sixth- and third-ranked risk, respectively, for 2024 and 2034. It is clear that the solution to growth is rooted in increasing productivity, not headcount. Embracing technology is part of the solution, particularly in countries where the working population is declining, immigration policy is not aligned with this reality and offshoring is giving way to re-shoring. These market forces necessitate the need for upskilling the existing workforce.
- **Rising labour costs continue to be a persistent concern.** Driven by shortages in skilled labour, increases in labour costs represent the ninth-ranked risk for both 2024 and 2034.
- **Broader return-to-work trends in the market, workplace evolution are less of an issue.** Managing

demands on or expectations of the workforce to work remotely or as part of a hybrid work environment fell to the 24th-ranked risk for 2024, down from ninth for 2023. Leaders are seeing more clearly how to deal with this issue as the workplace continues to evolve. They are adapting to a world profoundly affected by the pandemic experience, a world in which many exited the workforce, have rethought work-life balance and/or are re-entering the workforce with different priorities.

- **Culture-related risks have fallen in relative importance.** Resistance to change restricting the organisation from adjusting its business model and core operations fell from the fourth-ranked risk in both the 12-month and 10-year outlooks last year to 14th and 18th, respectively, this year. The organisation's culture not sufficiently encouraging timely identification and escalation of emerging risk issues fell from eighth to 17th in the 12-month outlook and from 16th to 21st in the 10-year outlook. These declines may be due to companies' emphasis on increasing organisational resilience and employees' risk awareness in a rapidly evolving business environment.

Third-party risks rise in importance.

Interestingly, relative to other risks, third-party risks increased from 17th and 15th in last year's 12-month and 10-year outlooks, respectively, to fourth and sixth for 2024 and 2034, respectively, in this year's survey. This increase is likely due to increasing reliance on outsourcing and strategic sourcing arrangements, ecosystem partners, IT vendor contracts, and other partnerships/joint ventures to achieve operational and go-to-market objectives. Cyber threats and regulatory compliance risks (e.g., data privacy regulations) also come into play here, as organisations must ensure their third-party vendors (as well as their third parties' vendors further downstream) are complying with current laws and regulations. It may also be attributable to the geopolitical climate, e.g., the West de-risking its reliance on China, laws and regulations restricting business activities and operations in certain countries, and other developments having implications that extend to an organisation's reliance on third parties. These interconnected risks highlight the importance for boards and C-suite executives to take a portfolio, enterprisewide view of oversight of emerging risks.

The spectre of regulatory changes and scrutiny — in wide-ranging industry-specific and pervasive areas — looms both near- and long-term.

Heightened regulatory changes and scrutiny increased relative to other risks, both near-term and long-term. This issue is the fifth-ranked risk overall for both 2024 and 2034, up from 16th and ninth overall in last year's 12-month and 10-year outlooks, respectively. As continued economic uncertainty increases the likelihood governments and various agencies will interfere with market functions through regulatory overreach and even excess, directors and C-suite leaders appear to perceive uncertainty over the likelihood and magnitude of forthcoming changes in the regulatory landscape that will affect their organisations. These concerns are often industry-specific. For example:

- In financial services, various regulations in different regions may increase capital and liquidity requirements and compliance costs, resulting in higher borrowing costs and reduced shareholder returns.
- Technology companies face increasing accountability for the impact of their innovations and products on consumers and the public, including the social implications of third-party content that misinforms and disinforms.
- Energy and utility organisations face scrutiny on the environmental impact from their production and use of fossil fuels.

In addition, a growing number of laws and regulations emerging around the world have pervasive impacts across industries. Examples include data privacy, climate disclosures, sustainability reporting, cyber breach disclosures, expanded attestation requirements and other matters, all of which may be elevating concerns among organisation leadership. Many of these pervasive issues fall to public companies. Accordingly, it is noteworthy that they were the only organisational type to report a slight increase in the overall magnitude and severity of risks for 2024.

Prior to the COVID-19 pandemic, regulatory risk was almost always rated a top 10 risk since this global survey began 12 years ago. Now that the pandemic is in the rearview mirror for most observers, regulatory uncertainty appears to have reclaimed its "rightful place" in the global risk profile.

The 10-year top risks outlook: More disruptive times lie ahead.

Long-term, the top risks landscape is relatively stable, as eight of the top 10 risks last year are on this year's top 10 list. However, risk levels longer-term are elevated over the 10-year outlook last year and the near-term outlook this year. Six of the risks are rated at the "Significant Impact" level (versus three last year). Risk issues of concern looking out 10 years include cyber threats, attracting and retaining top talent and labour and succession challenges, the need for new skills to fully deploy newly adopted digital technologies, rapid speed of disruptive innovation, evolving regulatory issues, the impact of third-party risks on business performance and brand image, uncertain economic conditions, the limiting obstruction of aged technical architecture, anticipated labour cost increases, and inability to deploy advanced data analytics (the "big data" problem).

This dynamic risk landscape and its elevated risk levels sustain the ongoing narrative that the 2020s are indeed a decade of disruption. With continued advances in AI, automation in all of its forms, ever-increasing connectivity, quantum computing, blockchain and digital currencies, and the metaverse, the market is likely to experience the largest wave of disruption since the turn of the century. This disruption will manifest itself in many ways, e.g., new business models, rapid product innovation, changing customer value propositions and disintermediation of distribution channels, and different needs for skills and talent. It will sweep away obsolete strategies, traditional moats, technical debt-laden architectures, conventional management playbooks and old school employee skills. The never-ending question every organisation faces in the global marketplace: Are we being disrupted and, if so, how and when would we know?

Data privacy and "big data" remain key areas of focus.

The complexity of the data privacy regulatory environment continues as a priority for organisations. Risks associated with data privacy are ranked 10th for 2024 and 11th for 2034, compared with being ranked 12th and fifth, respectively, for the 12-month and 10-year outlooks in last year's survey. Conversely, the risk of inability to utilise rigorous data analytics to achieve market intelligence and increase productivity and efficiency is ranked 10th overall looking out 10 years but is the 11th-ranked risk for 2024. Organisations successful in deploying forward-looking lead indicators and integrated analytics are likely to be more anticipatory and less reactive than those that aren't — and leaders know it. These capabilities generate the information and insights so essential to arming decision-makers with a time advantage in disruptive markets.

Climate change and sustainability risks have elevated.

Growing focus on climate change and other sustainability policies, regulations and expanding disclosure requirements as well as expectations of key stakeholders increased from the 28th-ranked risk looking out 12 months last year to the 22nd-ranked risk this year. Interestingly, looking out 10 years, this issue increased from the 20th-ranked risk last year to the 13th-ranked risk this year. Typically associated with existential planetary threats, climate- and sustainability-related risks are garnering more attention at a micro level by individual organisations relative to other risks. Growing regulatory focus (e.g., the Corporate Sustainability Reporting Directive in the EU) is likely to keep this risk issue on the radar long-term. Note that the focus on climate change and sustainability is the second highest-rated risk in Europe. Therefore, it is important that leadership teams in regions such as the U.S., where ESG is perceived as a polarising concept, not construe the regional view as representative of a global perspective.

Concerns over supply chain issues have subsided.

Uncertainty surrounding the core supply chain ecosystem is ranked 19th for 2024, quite a fall from ranking fifth in 2023. Many of the issues in the supply chain were a product of the disruption and congestion caused by the COVID-19 pandemic. These issues have been unwinding for some time. This risk was not viewed as a significant long-term concern last year and is not this year (ranked 25th looking out to 2034).

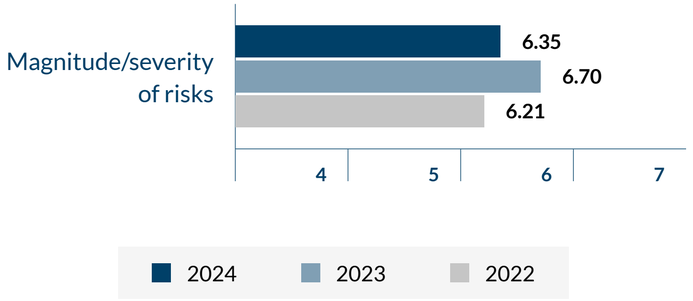
Risk levels declined from last year but remain higher than two years ago.

The participants were invited to rate the magnitude and severity of the total risk landscape impacting their organisations achieving performance goals over the next 12 months. On a 10-point scale, the overall ratings over the last three years are 6.35 looking forward to 2024, 6.70 for 2023 and 6.21 for 2022, as illustrated in Figure 1.

Of note, impressions of the magnitude and severity of the risk landscape organisations will face over the next 12 months showed some differences pre- and post-October 7, 2023, when the Israel-Gaza events erupted. The overall rating among responses collected before October 7 is 6.34, whereas it increased to 6.51 among responses collected after October 7.

FIGURE 1

Overall, what is your impression of the magnitude and severity of risks your organisation will be facing with respect to achieving your performance goals over the next 12 months?



Operational risks, both near term and long term, dominate the risk profile composition over macroeconomic and strategic risks.

Looking to 2024, eight of the top 15 risks are operational in nature and four are macroeconomic. Looking out 10 years, eight of the top 15 risks are operational in nature and the remaining seven are split between macroeconomic and strategic risks.

The largest elevated risk rankings for 2024 reflect a broad focus.

The four largest elevated risk rankings are the following (five risks tied for fifth and are not listed):

	From (2023)	To (2024)
Third-party risks	17th	4th
Sustaining customer loyalty and retention	25th	12th
Cyber threats	15th	3rd
Heightened regulatory changes and scrutiny	16th	5th

These increased risk ratings reflect elevated concerns on various strategic and operational fronts and underscore the increasing complexity of the evolving risk landscape.

There is significant churn in the top risks near-term.

Six of last year's top risks looking out 12 months fell out of this year's top 10 list for 2024.

	From (2023)	To (2024)
Resistance to change	4th	14th
Managing uncertainty surrounding supply chain ecosystem	5th	19th
Impact of changes in work environment on culture	6th	15th
Culture not supporting timely escalation of risks	8th	17th
Managing workforce expectations of hybrid work environment	9th	24th
Not sufficiently resilient or agile responding to a crisis	10th	16th

These risk issues were replaced with risks associated with cyber threats, third-party risks, heightened regulatory changes and scrutiny, exposure to nimbler competitors (including those that are either "born digital" or investing heavily to leverage technology for competitive advantage), changes in the interest rate environment, and ensuring data privacy and compliance with proliferating identity protection expectations and regulations.

The five largest elevated rankings in risks looking out 10 years are also mixed.

The five largest elevated rankings in risks looking out 10 years are summarised below (two risks tied for fifth):

	From (2023)	To (2024)
Cyber attacks	13th	1st
Third-party risks	15th	6th
Impact of changes in work environment on culture	22nd	14th
Geopolitical shifts, regional conflicts and political instability	31st	23rd
Growing focus on climate change and other sustainability policies, regulations, and expanding disclosure requirements as well as expectations of key stakeholders	20th	13th
Change in current interest rate environment	26th	19th

The above risks reflect a mix of macroeconomic, strategic and operational concerns. Interestingly, the reference to geopolitical shifts and regional conflicts presages the developments in the Middle East commencing in the last week our survey was open. As indicated earlier, we noticed an uptick in this risk during that week.

The top 10 risks for both 2024 and a decade later (2034) are highlighted in the charts that follow. As indicated by the red arrows, three of the top 10 risks for 2024 are rated higher than they were for 2023, and nine of the 10 top risks for 2034 are higher than last year's survey that also looked out a decade. Eight of the top 10 risks for 2024 remain top 10 risk concerns a decade from now.

Top 10 risks for 2024		
1. Economic conditions, including inflationary pressures	5.96	↓
2. Ability to attract, develop and retain top talent, manage shifts in labour expectations, and address succession challenges	5.93	↓
3. Cyber threats	5.90	↑
4. Third-party risks	5.63	↑
5. Heightened regulatory changes and scrutiny	5.61	↑
6. Adoption of digital technologies requiring new skills in short supply	5.52	↓
7. Existing operations and legacy IT infrastructure unable to meet performance expectations as well as "born digital" competitors	5.51	↓
8. Change in current interest rate environment	5.48	↓
9. Increases in labour costs	5.48	↓
10. Ensuring privacy and compliance with growing identity protection expectations	5.43	↓

Top 10 risks for 2034		
1. Cyber threats	6.44	↑
2. Ability to attract, develop and retain top talent, manage shifts in labour expectations, and address succession challenges	6.27	↑
3. Adoption of digital technologies requiring new skills in short supply	6.16	↑
4. Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces	6.15	↑
5. Heightened regulatory changes and scrutiny	6.13	↑
6. Third-party risks	6.00	↑
7. Economic conditions, including inflationary pressures	5.95	↑
8. Existing operations and legacy IT infrastructure unable to meet performance expectations as well as "born digital" competitors	5.91	↑
9. Increases in labour costs	5.87	↑
10. Inability to utilise rigorous data analytics to achieve market intelligence and increase productivity and efficiency	5.79	↓

A series of calls to action

The ever-changing risk landscape and the overall perceived magnitude and severity of risks should prompt boards and senior executives to scrutinise closely the approaches they use to remain focused on emerging risk issues and to integrate those insights into strategic decision-making. Now may be an opportune time for boards and C-suites to examine closely where to invest not only to preserve market image and branding but also foster a strong recovery when the economy bounces back and prospects for growth improve.

Given the long-term risk landscape, the question arises: What steps should be undertaken or continued over the near term to ensure the organisation is sufficiently agile and resilient to thrive in a decade of disruption?

To help facilitate consideration of next steps, we present the following calls to action that executives and directors can consider when evaluating their organisation's readiness for the future as they cope with near-term business realities. We have centred these calls for actions along these key themes:

- Navigating an uncertain economic environment
- The cyber issues executives should be thinking about
- Forging ahead with artificial intelligence capabilities
- Embracing new talent strategies
- Understanding and managing the geopolitical risk landscape

These calls to action are not intended to be a comprehensive list of themes. They highlight issues common to most organisations that are worthy of further consideration and analysis. We also include a diagnostic in this report to assist companies in evaluating how they approach risk management and oversight in the digital age. It can be used to identify areas in which to improve risk assessment and risk management processes.

Navigating an uncertain economic environment in 2024

BY CHRIS WRIGHT
GLOBAL LEADER, BUSINESS PERFORMANCE IMPROVEMENT SOLUTIONS, PROTIVITI

Despite continued optimism in some quarters that a severe recession can be avoided and recent evidence that the pace of inflation may be slowing, our survey results show the economy as the top risk entering 2024. Because no one knows for sure what's going to transpire, we expect this risk to continue to be on the minds of executives throughout 2024. A fluid inflation dynamic leaves the market with uncertainty about the direction of central bank policies, geopolitical transitions that could make inflation sticky and the reality that many leaders haven't faced an inflationary economy in their entire careers.

Following are recommended steps for navigating this uncertain environment.

Focus on generating reliable information for decision-making. Companies should deploy multiple, reliable and objective sources of historical and forecasted economic, inflation and related capital markets data. Key performance indicators and reliable reporting on customer, supplier, employee, lender, competitor and investor actions should be developed. Data sources should be given the same rigorous review management would ordinarily give to inbound and outbound cash flow requests. They deserve that high of a priority.

Build a reliable forecasting (and reforecasting) capability. An inflationary and uncertain economic environment merits a dynamic forecasting and budgeting process. It should consider such market-driven factors as:

- Impact of the economy on customer buying behaviours;
- Inflationary pressures on labour costs and employee mobility;
- Inflationary pressures on critical materials, components and supplies; and
- Inflation-fighting monetary policy impacts on the cost of capital.

The forecasting and planning process should be objective and as free of bias and unplausible assumptions as possible. Quality real-time market data deters excessive reliance on historical data and trends when those trends may not hold up in the face of new and emerging realities. Alternative scenarios of alternative futures enable stress tests of top-line performance, operating costs and cash flows.

Monitor your (and your customers' and vendors') financial strength, credit capacity and behaviour. Depending on the magnitude of a downturn, should one occur, companies should prepare and undertake a hierarchy of initiatives to manage margins through headcount reductions; compensation adjustments; reductions in selling, general and administrative expenses; cessation of expansion plans; effective hedging strategies; and discontinuance of underperforming operations, products and services. They should monitor and enforce approaches to minimising customer credit losses. They should also have a "Plan B" (or B, C and D) for sourcing critical materials, components and supplies in the event of economic disruptions of the supply chain. Finally, they should understand where they stand with lenders and shareholders with intention to preserve financial health.

Don't forget your employees. With the economy and inflation having an impact on employee anxiety, satisfaction and termination/retention decisions, straight talk and transparent communications are necessary to preserve morale and trust. No news does not necessarily mean good news. Of particular importance is the impact of economic forecasts, company operating performance and inflation on compensation expectations.

In uncertain times, the above steps will help executives and directors develop a response plan to deal with economic headwinds. Created in the cool of the day, the company will be more prepared and resilient should a downturn occur.

The cyber issues executives should be thinking about in 2024

BY SAMEER ANSARI
GLOBAL LEADER, SECURITY AND PRIVACY PRACTICE, PROTIVITI

As organisations continue to push their digital agenda, their data proliferates across the enterprise as well as outside their physical boundaries, and their attack surface continues to expand, cybersecurity presents a top-of-mind risk for executives and directors. Rather than rehash the table stakes of a strong cybersecurity framework, we offer the following actions for leaders to consider as they enter 2024.

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 move toward digitisation, 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 really 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. The time is now for organisations to think about how they can 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, much like the recent executive order in the United States, 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, while also making sure they don't obstruct their business strategy.

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.

Forging ahead with artificial intelligence capabilities in 2024

BY CHRISTINE LIVINGSTON
GLOBAL LEADER, ARTIFICIAL INTELLIGENCE SERVICES, PROTIVITI

A global IBM survey of 3,000 CEOs indicated that half (50%) are already integrating generative AI (GenAI) into digital products and services. Many are also concerned about data security (57%) and bias or data accuracy (48%). Only 28% have assessed the potential impact of GenAI on their workforces, and 36% plan to do so in 2024. Interestingly, seven of 10 non-CEO senior executives report that their organisation is not ready to adopt GenAI responsibly. With this backdrop, following are steps leaders should take:

Identify opportunities for AI and GenAI now. Despite the challenges and uncertainties of GenAI, business leaders should be eager to seize the opportunities offered or else risk their businesses being disrupted. The risk of doing nothing is greater than the risk of doing something.

Authorise an autonomous cross-functional team to review opportunities and formulate a strategy. Empower it with a shared vision giving it purpose, e.g., improve the customer experience or reimagine operational processes. In addition to thinking big and being disruptive, the team should:

- Be multidisciplinary, while being nimble enough to support rapid decision-making;
- Explore how GenAI is being used across industries;
- Identify practical opportunities that are aligned with overall business objectives and the stated vision for AI and can drive meaningful business value; and
- Educate key individuals at an appropriate depth according to their expected contributions, and put the onus on these individuals to educate a larger group of people in the organisation.

Absent significant expertise in GenAI capabilities, increasingly corporations are seeking external assistance to guide initiatives and support initial development.

Establish a framework for evaluating use cases and managing risk. Once the team has defined potential concepts and use cases, each should be evaluated for feasibility and complexity while also considering the availability of technologies to achieve desired outcomes. The team should:

- Evaluate the business benefit, architectural requirements, data integrations, security issues, and governance and compliance implications;
- Develop specific value measures expected from each selected pilot use case, with an eye for future unanticipated value; and
- Outline an anticipatory road map to optimise investments and visualise correlations and reusability across use cases.

Leveraging GenAI capabilities requires leaders to develop ethical and responsible governance frameworks (to, among other things, ensure appropriate human involvement in critical decisions) and begin the journey with innovative pilots.

Initiate pilots to confirm viability and demonstrate value. The team should facilitate the creation of AI-enabled prototypes to confirm that the concepts identified are technically viable, the data is sufficient, and that they demonstrate a path to delivering business value, exploring and tuning the model(s) iteratively to deploy pilot solutions. Establish business value metrics and KPIs to benchmark and monitor. Automating metrics and monitoring enables data-driven decisions about subsequent enhancements and possible future AI initiatives. Evaluations of the development process and the application itself result in improvements as the iterative process continues.

Understanding the opportunities, limitations and risks of these models is a strategic imperative. Companies will be most successful and unleash the most potential when infusing GenAI capabilities with their own proprietary data and documents.

Embracing new talent strategies in 2024 and beyond

BY FRAN MAXWELL
GLOBAL LEADER, PEOPLE ADVISORY & ORGANISATIONAL CHANGE, PROTIVITI

Talent-related issues proliferate the top 10 global risks for both 2024 and the next decade. Attracting, developing and retaining top talent qualifies as a prevalent, pressing risk in an era when an organisation's people greatly influence how well it addresses other top risk concerns, including cyber threats, the adoption of digital technologies and advanced tools (e.g., generative AI), third-party risks, and organisational resilience and agility, among many others. This makes it imperative for boards, CHROs and other C-suite leaders to reinvent their talent strategies through the following actions:

Adopt a new talent mindset. Your organisation cannot rely on the ability to "go hire more" data scientists, nurses, systems architects, AI specialists, or other in-demand talent whenever it wants. Such types of prized skills are not widely available. Nor can you afford the costs and culture risks associated with yo-yoing between hiring binges and layoffs. A modern talent mindset:

- Focuses on the skills instead of roles or jobs;
- Prioritises the value talent generates over its cost;
- Sources skills from a diverse and flexible talent pool of full-time employees, contract and temporary workers, expert external consultants, and managed services and outsourcing providers;
- Treats leadership development and succession planning as a shared responsibility among all leaders;
- Leverages a resilient and innovative organisational culture as a recruiting and retention advantage.

Align the talent mindset with business strategy. As organisational performance becomes increasingly reliant on the quality of people and teams, it is crucial to ensure the talent strategy aligns with the business strategy. Both game plans should remain in lockstep as strategic objectives change and as new opportunities and threats arise with greater frequency.

Take a talent inventory, assess, respond and repeat. Perform regular assessments of the organisation'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 of the skills that reside throughout the enterprise. Evaluate these talent inventories based on their alignment with longer-term business objectives. When skill gaps arise, develop strategies to close them. Distill these assessments and corrective actions into the periodic reports the CHRO delivers to the board.

Institute rolling talent forecasts and analyse the financial impacts of talent scenarios. HR groups should take a page from FP&A teams by deploying a rolling forecast that focuses on the skills (in addition to headcounts) needed to execute strategic business objectives. By modelling the impact of different external factors (e.g., labour cost increases) and strategic changes (e.g., investing in generative AI) on the organisation's skills requirements, HR leaders, working closely with business leaders, can identify future skills needs and quantify the financial impact of various scenarios.

Deploy new skills analytics. Measure and report on open positions, skills at risk, upskilling opportunities, DEI- and ESG-related metrics relevant to business objectives, and the health of the organisation's culture (e.g., well-being indicators). These metrics help the C-suite monitor organisational effectiveness, which is the extent to which the workforce is delivering on strategic objectives.

Understanding and managing the geopolitical risk landscape

BY CAROL BEAUMIER
SENIOR MANAGING DIRECTOR, RISK AND COMPLIANCE, PROTIVITI

Geopolitical risks occur as a result of a shift in power, a conflict or a crisis. The effects of geopolitical risk may be political, economic, societal (including environment, health and safety), legal and regulatory. These risks also impact cybersecurity. With conflicts and tensions currently spanning multiple continents and recent and upcoming elections potentially reshaping global politics, the following are important considerations for the board and the C-suite:

Don't think that you are isolated from geopolitical risk. Those affected by geopolitical risk include not only large multinational companies that may find themselves in the middle of the fray, but also midsize and smaller companies across the globe that may experience a wide range of downstream consequences, including but not limited to commodity prices or shortages.

Stay informed. The complexities of the geopolitical environment may mean that general knowledge of world events is likely not sufficient to predict the consequences. Enlist the assistance of well-trained advisers who can offer advice based on experience, research and deeper market intelligence that may not be available to most individual companies.

Include geopolitical risk in your enterprisewide risk assessment. Consider and evaluate, through scenario analyses, the potential implications of the changing geopolitical landscape for the business and for customers of the business. Keep in mind that comprehensive scenario analyses may require considering the consequences of more than one geopolitical event occurring simultaneously and that assessment of geopolitical risk must be dynamic.

Develop contingency and resilience plans. Know what your course of action will be if geopolitical developments alter your business strategy or operations — at least plan for the developments that are most likely or that would have the most significant impact on your company.

Be mindful of escalating legal, credit and reputation risks. Following the Russian invasion of Ukraine, Western allies quickly and in a heretofore unprecedented manner turned to economic sanctions in an effort to punish Russia for its actions. While there was broad agreement on the principles of whom and what should be sanctioned, national and regional sanction regimes rolled out the sanctions in different ways, creating significant compliance challenges and reputation risk for companies with direct Russian exposure or exposure through their customers. It is reasonable to expect that economic sanctions will continue to be used in other circumstances as public policy tools. And remember that sanctions imposed are often retaliated, creating legal and credit risk challenges for companies (or their customers) trying to unwind their exposure.

Consider your response. How a company responds, or whether it responds at all, to geopolitical events has become a lightning rod for controversy and criticism. While every geopolitical event cannot be anticipated, the board and the C-suite should define in advance the circumstances that would prompt messaging about an event to the organisation (i.e., internally) or to the broader market, and should outline the parameters of the response.

Geopolitical risks are a global threat to business with no signs of abating in the near future. Managing these risks effectively should be a core competency for all businesses.

Highlights of key differences across subsets of respondents

What you need to know

Risk perceptions vary by organisation size: For 2024, organisations perceive a slight decrease in risk magnitude and severity compared to 2023, but overall assessments are higher than two years earlier.

- Concerns in 2024 about economic conditions, talent and cyber threats are common across all size groups.
- Regulatory change is a top risk for larger organisations in 2024 and is the top overall risk for this group looking out to 2034.
- Third-party risks are notable for midsize organisations.
- Smaller organisations face hurdles in adopting digital technologies due to the size of the talent pool.
- Long-term risk concerns are higher than near-term concerns for organisations of all sizes.
- Technology-themed risks dominate the list for the next decade.

Across executive positions, risks are expected to decrease somewhat in significance for 2024 relative to 2023, but are rated higher than 2022. CAEs have the highest perception of risk. CEOs and boards agree on the significance of risks. CFOs are the most optimistic.

- Economic and talent concerns are common across all positions.
- Long-term risk concerns vary.

Most industries rate risks lower for 2024, but overall concerns remain significant. Industry-specific risks vary.

- There is marked contrast in perspectives across industry groups about specific risk concerns.
- Cyber threats and talent concerns are common top five risks across most industries for both 2024 and 2034.
- Most industry groups rank concerns about economic conditions, including inflationary pressures, as a top five risk concern for 2024.
- Healthcare rates the most risks in 2024 as "Significant Impact."

Views on risks and risk levels vary across regions. Succession planning and talent concerns are common issues. Cyber threats and economic conditions are top risks. Strategic risk concerns are more common long-term.

Public companies report increased risks for 2024. Top risks are reasonably consistent across entity types, with the most distinctive risk profile being private companies with plans to go public. Not-for-profit and government entities have high risk concerns. Long-term risks increase for all types, with cyber threats, rapid speed of digital innovations and the need to upskill to deploy digital technologies as the top concerns.

Investment in risk management is not likely to be higher in 2024 than 2023.

- Boards and executives need to adapt to the changing risk landscape and increase transparency.

What's next: Boards and executives need to evaluate their risk management approaches and monitor and address emerging risks proactively.

In addition to presenting overall risk insights from the 1,143 respondents, later sections of this report provide insights from the analysis of findings across different dimensions, including size of organisation, the leadership positions of respondents in the organisation, industry group, geographic regions, and organisation type (public, private, not-for-profit or government).

Differences across sizes of organisations

- Organisations of all sizes perceive a slight decrease in the magnitude and severity of risks in 2024 for their organisations in comparison to 2023, but their overall assessments of magnitude and severity of risks are higher relative to two years earlier. While this suggests some general improvement in risk conditions, in general caution still remains. Organisations with revenues between $100 million and $999 million perceive their overall business environment to be riskier relative to all other sizes of organisations, with an impact score of 6.52.
- What is striking for 2024 is the generally higher level of risk concerns for the two categories of smaller organisations (those with revenues below $1 billion). In both categories, respondents rated all of their top five risks as higher in 2024 relative to 2023. Collectively, this suggests smaller-sized organisations perceive the risk environment as more impactful for them near term relative to larger organisations.
- Three risks are common top five risks across all size groups for 2024: (1) Concerns about attracting and retaining talent, including succession challenges; (2) concerns that economic conditions (and inflationary pressures) in markets served may affect growth and profitability; and (3) concerns about cyber threats. Except for the largest-sized organisations, concerns about economic conditions represent the top- or second-ranked risk across all organisations, while attracting talent and cyber threats are of greater concern for the largest organisations. Cybersecurity concerns are higher in the top five list of risks for the two largest-sized organisation categories relative to smaller organisations. The visibility of larger organisations may make them a greater potential target for cyber disruption.
- Concerns about heightened regulatory changes and scrutiny are a top five risk for the two largest size categories of organisations for both 2024 and looking out to 2034. The higher impact of this risk on larger organisations may be linked to recent regulations related to the climate-related disclosure rules in the European Union (and pending SEC climate disclosure rules in the United States) as well as required cyber breach disclosures, potential expansion of attestation requirements, and other matters that the largest organisations perceive affect them the most.
- Third-party risks made the list of top five risk concerns for the two organisation size groups in the middle range for 2024. Perhaps reliance on third-party partners and

"Current economic conditions are proving to make short- and long-term outlooks as difficult to predict as they have been at any time over the past 50 years. Unemployment rates continue to hover near historic lows and consumer spending remains robust, despite traditional indicators such as inflationary trends and higher interest rates that would suggest the opposite should be happening. Given the level of uncertainty for the foreseeable future, especially with a volatile geopolitical climate further clouding economic forecasts, boards and management need to focus on assessing the right data, metrics and KPIs to assess the health of their business on a continuous basis and pivot with agility when necessary."

DR. PETER HENRY
SENIOR FELLOW, HOOVER INSTITUTION & FREEMAN SPOGLI INSTITUTE, STANFORD UNIVERSITY; INDEPENDENT DIRECTOR; PROTIVITI ADVISORY BOARD MEMBER

vendors is more notable for these organisations as they seek growth opportunities over time.

- The two categories of smaller-sized organisations rated perceived lack of skills needed for their adoption of digital technologies as a top five risk. Given the size of the talent pool, smaller organisations may face greater hurdles in embracing emerging innovation as they compete for talent to help them leverage the advantages and fully realise the value proposition offered by new innovation opportunities.
- The differences in perceptions about long-term (2034) risk conditions relative to near-term (2024) risk concerns is noticeable. In each of the four organisation size categories, respondents rated all top five risks at "Significant Impact" levels, suggesting that their concerns about 2034 are of a higher risk level relative to their near-term risk concerns. Additionally, the two smaller size categories of organisations rate all of their top five long-term risks higher than their assessments of long-term risks revealed in last year's study. Clearly, respondents are expressing greater pause about long-term outlooks this year relative to their outlooks last year.
- Technology-themed risks seem to dominate the list of top risks for a decade from now. All sizes of organisations rate cyber threats as a top five risk, with all except the very largest size category rating that concern as their number one risk issue. Concerns about the ability to adopt emerging digital technologies also is in the top five risks for all organisations, and risks related to the rapid speed of disruptive innovations enabled by new and emerging technologies made the top five risks for all sizes of organisations, except the smallest size category.

Differences across executive positions represented

- The overall impression across different executive positions with respect to the magnitude and severity of risks in the environment is that risks are decreasing for 2024 over 2023. The one exception is for chief audit executives (CAEs), whose assessment did not change between 2023 and 2024. It is worth noting that CAEs have the highest perception of the magnitude and severity of risks relative to all other executive positions. While there is a decrease in risk levels from last year, most executive positions rate the overall magnitude and severity of risk conditions for 2024 to be at the "Significant Impact" level. Thus, the risk environment continues to be an important overarching issue for executives and boards to navigate. Only chief strategy/innovation officers (CSOs) and chief data/digital officers (CDOs) rate the magnitude and severity of overall risk conditions below that level for 2024.
- While CEOs rate the overall magnitude and severity of risk conditions for 2024 higher than board members do, both rate that overall concern at the "Significant Impact" level. There is general agreement in the relative significance among specific risks between CEOs and boards, given all of the 36 risks are rated at the

The overall impression across different executive positions with respect to the magnitude and severity of risks in the environment is that risks are decreasing for 2024 over 2023.

"Potential Impact" level (4.51 through 5.99) by both CEOs and boards, except for one risk that CEOs rate at the "Less Significant Impact" level (4.50 or lower).

- Chief risk officers (CROs), CAEs and chief human resources officers (CHROs) see individual risks differently for 2024, with each executive position rating at least five of the 36 risks for 2024 at the "Significant Impact" level, whereas no other executive position rates risks at that level of impact. Interestingly, there is variation across those three groups as to the risks that rank at that level, suggesting they see differences in the relative significance of specific risks. CFOs are the most optimistic about 2024, given they rate nine of the 36 risks at the "Less Significant Impact" level.

- Most positions identify risks related to attracting and developing talent and risks related to the economy as top five risks, with eight of 10 executive positions including those two risks in their top five risk concerns. Interestingly, CHROs did not include concerns related to attracting talent as a top five risk concern. CSOs and CDOs are the only two positions to not identify the economy as a top five risk issue.

- There is general agreement among boards and CEOs in the specific issues included in their top five risks in 2034, given four of the top five risks are the same for both positions. CFOs have somewhat differing views about the top risks compared to boards and CEOs, given CFOs are the only one out of those three positions to highlight concerns related to labour costs and the changing current interest rate environment as top five risk issues. This is not surprising as CFOs are always focused on market factors that can impact the bottom line. CEOs are the only ones among those three positions to identify risks related to heightened regulatory changes and scrutiny, reflecting their sensitivity to potential constraints on the business model and strategy.

- For a decade out (2034), overall risk perceptions exhibit significant variation relative to 2024. Board members rate three of their top five risk issues at the "Significant Impact" level, while CEOs, CFOs and CROs rate none of their top five risks at that level. CAEs have the most concern about the future, rating 15 risks at the "Significant Impact" level, including eight of the 14 operational risks — an important point given that operations are a key point of focus in many audit plans. The 2034 results show an increase in overall risk concerns relative to short-term risk concerns.

- As noted earlier, there is general agreement in long-term top five risks for boards and CEOs, with technology-themed risks comprising three of their top five risk issues. Additionally, all executive positions — except CFOs — include cyber threats as a long-term top five risk, with six of 10 positions rating that risk in the number one or two position for a decade later. Eight of 10 executive positions also include concerns about the adoption of digital technologies requiring skills in short supply as a top five risk concern 10 years from now. Six of 10 positions include concerns about the rapid speed of disruptive innovation as a top five long-term risk concern.

"It should be of no surprise to find that talent and workforce issues are prevalent themes in the lists of top risks for 2024 and the next decade. From retention and succession planning challenges to upskilling to meet the next wave of innovations and emerging technologies, organisations face mounting concerns that they will be unable to bring in the talent and skills needed to compete. Compounding these challenges is the approaching wave of retirement of a baby boomer generation of people that will leave a sizable gap in the workforce."

DAME INGA BEALE
INDEPENDENT DIRECTOR,
PROTIVITI ADVISORY BOARD MEMBER

Differences across industry groups

- Most industry groups rate the overall magnitude and severity of risks for 2024 somewhat lower than their ratings for 2023, except for the Energy and Utilities and Manufacturing and Distribution industry groups, which rate 2024 risks higher than 2023. Despite slight reductions from prior year levels, respondents across all industry groups perceive the overall magnitude and severity of risks to be at the "Significant Impact" level, except for government-related entities.

- With the continuing transitions happening in the energy sector, it is not surprising that Energy and Utilities respondents believe that 2024 will be riskier than 2023, even though none of the 36 risks is rated by this industry group at the "Significant Impact" level and 10 are at the "Less Significant Impact" level (4.50 or lower). The rating of 10 of the 36 risks as "Less Significant Impact" by Energy and Utilities respondents is more than any other industry group.

- There is a marked contrast in perspectives across industry groups about specific risk concerns, supporting the view that industry context is important to consider. But given that certain types of organisations' business models may not fit neatly into a single industry category, reviewing differences in risk concerns across multiple industries may help tease out risks that otherwise could be overlooked.

- Healthcare industry respondents rate the most risks at the "Significant Impact" level, with seven rated at that level for 2024. Four of their seven highest-rated risks are operational in nature, with specific concerns noted related to cyber threats, data privacy, third-party risks and talent shortages (most likely clinical healthcare workers, particularly nurses). Financial services respondents rate four of the 36 risks at the "Significant Impact" level, with two of those four relating to overall economic conditions and the current interest rate environment (both macroeconomic issues), one related to heightened regulatory scrutiny, and one related to cyber threats.

- Three of the seven industry groups rate cyber threats at the "Significant Impact" level: Financial Services; Technology, Media and Telecommunications; and Healthcare. Financial Services, Consumer Products and Services, and Healthcare are all concerned about economic conditions, including inflationary pressures. Financial Services and Healthcare are the two industries most concerned about heightened regulatory scrutiny.

- All industry groups rate cyber threats as a top five risk concern, suggesting no industry is immune to those exposures. All industries, except Energy and Utilities and Government, include concerns about economic conditions, including inflationary pressures, as a top five risk concern for 2024. And all industries, except Financial Services, highlight concerns about the ability to attract, develop and retain talent as a top five risk concern for 2024. Increases in labour costs are of particular concern for Healthcare, Consumer Products and Services, and Government for 2024.

"The fact that cyber threats are a critical risk next year and in the next decade is not a new revelation, but it does not diminish its importance or the threats that cyber attacks pose, especially over the long term. Given the increasing sophistication of technologies used to execute these attacks and their expected maturity by 2034, and particularly considering the rise of AI, most organisations likely see a cyber attack and/or breach as an inevitability. The question becomes what organisations should do about it. In short, they need the right people and skills to bolster cyber defences, they need effective data governance and management practices, and they need to reduce or eliminate the technical debt that elevates their cyber risk."

ADMIRAL DANELLE BARRETT
INDEPENDENT DIRECTOR,
PROTIVITI ADVISORY BOARD MEMBER

- The significance of risk concerns a decade out is noticeably higher than short-term risk concerns across the various industry groups. For five of the seven industry groups, all of the top five risks for 2034 are at the "Significant Impact" level. This is in contrast to the short-term outlook for 2024, where only one industry group (Healthcare) rated all top five risks at that level.
- Cyber threats are in the top five long-term risks for all industry groups, as are concerns about attracting, developing and retaining top talent, including succession challenges. Four of seven industry groups are concerned about heightened regulatory changes and scrutiny. That is the number one long-term concern for Energy and Utilities organisations.
- Rising threat of catastrophic natural disasters and weather phenomena is a top five long-term risk concern for Energy and Utilities organisations and Government Agencies. Consistent with prior years, the Energy and Utilities industry group rates a growing focus on climate change and other sustainability policies as a top risk concern. In addition, for the first time, the Manufacturing and Distribution industry group rated this risk as a top five long-term risk.

Differences across geographic regions

- Globally, organisations from seven of the eight geographic regions in our study agree that the overall magnitude and severity of risks are of a "Significant Impact" nature for 2024. Four rate the overall severity and magnitude of risks for 2024 as higher than 2023, which is remarkable given that 2023 overall registered the highest result on this question we have observed in the 12 years we have conducted this study.
- There are notable differences in views about risks around the globe, which is especially important for multinational organisations to consider. Respondents in North America, the Middle East and Africa rate at least three of their top five risks at the "Significant Impact" level, while Asia, India and Latin America do not rate any risks this highly.
- There is variation in the nature and types of risks included in the top five risks for the eight geographic regions. Fifteen of the 36 risks appear as top five risks among the eight geographic regions and seven of the eight regions report at least three operational risks in their top five for 2024.
- All eight geographic regions include concerns about succession planning and talent acquisition and retention as a top five risk, and three report it as their top-ranked risk concern for 2024. Macroeconomic risks related to economic conditions and cyber threats are both ranked in the top five risks in six of the eight regions.
- Looking ahead to 2034, strategic risks become more common in the top five risk concerns. The two most commonly cited top five concerns, each appearing in seven of the eight regions, are the risk associated with the adoption of digital technologies with its implications to the reskilling and upskilling of existing employees and the risk associated with cyber threats.

The significance of risk concerns a decade out is noticeably higher than short-term risk concerns across the various industry groups.

Differences across public and non-public entities

- For the three types of entities — publicly traded, privately held with no IPO plans, and private companies with plans for an IPO — for which we have comparative data, only public companies report a slight increase in the overall magnitude and severity of risks for 2024. All five organisations rate that overarching concern at the "Significant Impact" level.
- While we separately analyse publicly traded companies, privately held entities with plans for an IPO, privately held entities with no plans for an IPO, not-for-profit entities, and governmental organisations, we find that the top five risks across the five groups are reasonably consistent. Concerns related to succession planning and talent acquisition and retention are a top three risk concern for all groups. Concerns over economic conditions and cyber threats are in the top five list of risks for four of the five groups for 2024.
- Public companies are concerned about uncertainties related to increased regulatory change and enhanced scrutiny, the current interest rate environment, and the adoption of digital technologies and the related need to reskill and upskill employees. Private entities hoping to soon go public rate all five of their top five risks at the "Significant Impact" level, while public companies do not rate any of their top five risks at that level.
- Privately held entities with plans for going public are particularly concerned about organisational risk culture and privacy. Privately held entities (both those pursuing and not pursuing an IPO) also are focused on risks associated with third parties.
- Not-for-profit entities rate all five of their top risks at the "Significant Impact" level. Governmental organisations rate three of their five top risks at this level. Challenges associated with escalating labour costs are of particular concern for both, with that risk appearing in the top five for both types of entities.
- Interestingly, when looking a decade ahead, there appears to be an overall heightened level of concern. All of the top five risks are rated at the "Significant Impact" level for 2034 for each type of organisation, except for private companies with IPO plans. For this group, only one risk is rated this highly.
- For 2034, all five organisation groups are concerned about cyber threats, rating that risk in their top five. Except for private entities planning an IPO, all groups are also focused on risks for 2034 related to the rapid speed of disruptive innovations, succession challenges and talent acquisition and retention, and the need to upskill to deploy digital technologies. Private entities planning for an IPO are primarily concerned about risks related to growth strategies dependent upon M&A, increasing labour costs, third-party risks, and the effects of social media, along with cyber threats.

Public companies are concerned about uncertainties related to increased regulatory change and enhanced scrutiny, the current interest rate environment, and the adoption of digital technologies and the related need to reskill and upskill employees.

Plans to improve risk management capabilities

In addition to asking respondents to rate each of the 36 risks for 2024 and 2034, we asked them to provide insights about plans to enhance their organisation's risk management capabilities in the coming year. Here are some key insights:

- In light of the finding that respondents report a decrease in their impressions about the magnitude and severity of overall risks for 2024 relative to the prior year, they also indicate a lower likelihood of deploying more resources to risk management in 2024 relative to 2023 (and 2022). This result is not too surprising, especially considering the increased investment that has likely already occurred due to learning experiences from navigating through the pandemic.
- All groups of organisations based on size indicate they are less likely to strengthen their risk management processes in 2024 as compared to 2023. However, organisations of all sizes still rate this likelihood at 6.0 or higher. In a similar vein, all executive positions signal a lessened need for increased investment in risk management in the coming year.
- No industry group indicates an increased likelihood for investment in risk management from 2023 to 2024. The Financial Services industry group indicates the highest likelihood for 2024 (6.59). Energy and Utilities is the only industry group with a status quo outlook related to investment in risk management infrastructure, with the score declining by only a marginal amount from 2023 (6.19) to 2024 (6.10).
- Organisations based in Asia, Australia/New Zealand, and the Middle East indicate an increase in likelihood they will invest more in risk management capabilities in 2024 relative to our 2023 results, with respondents in India reflecting the highest overall likelihood for greater investment (a result that was also the case in 2023).
- All types of entities indicate lower levels of likelihood that they will invest more time and energy in building out their risk management infrastructure in 2024 relative to 2023. This result applies for those organisation types where we have comparative data for prior years. Still, all organisation types report a likelihood of increased investment at the 6.0 level or higher.

The ever-changing risk landscape and the overall perceived magnitude and severity of risks should prompt boards and senior executives to scrutinise closely the approaches they use to keep an anticipatory eye on emerging risks. Unfortunately, some organisations continue to manage risks the way they have for many years, even though the profile of risks is changing dramatically as businesses and entire industries are transformed in the digital economy.

The need for greater transparency about the nature and magnitude of risks undertaken in executing an organisation's corporate strategy continues to be high as expectations of key stakeholders regarding strategic relevance, risk management and risk oversight remain strong. At the end of this report, we offer a number of diagnostic questions for executives and boards to consider as they evaluate their organisations' approach to managing risks. It is our desire that this report will increase executive and board understanding of potential risks on the near- and long-term horizons. We also hope that this understanding will help leaders proactively navigate emerging issues and challenges for the benefit of their organisation's reputation and brand image, key stakeholders, and society as a whole.

The ever-changing risk landscape and the overall perceived magnitude and severity of risks should prompt boards and senior executives to scrutinise closely the approaches they use to keep an anticipatory eye on emerging risks.

The top risk concerns for 2024

What you need to know

By the numbers: Five of the top 10 risks are operational in nature, with four additional risks tied to macroeconomic concerns. Only one strategic risk falls in the top 10.

- Three of the top 10 risks are rated higher than they were rated in 2023: cyber threats, third-party risks, and heightened regulatory change and scrutiny.

There are overarching concerns about economic conditions and ongoing inflationary pressures.

Uncertainties persist about policy decisions among central banks, coupled with concerns about the current interest rate environment.

- These may reflect worries about how the overall economy may restrict growth opportunities and squeeze margins as operating costs and the cost of capital are higher relative to the past several years.

Talent concerns remain: There are challenges related to the labour market, particularly rising labour costs and difficulties in attracting unique skills needed to adopt emerging digital technologies successfully.

- Ongoing frustrations around compensation, managing flexible work options and other workplace challenges continue to create challenges in attracting and retaining the right talent needed for strategic success.
- Higher labour costs impacting profitability expectations are being driven by robust employment and skilled labour shortages.

Five of the top 10 risks link to business process challenges.

- Technology-dependent operations to ensure appropriate cybersecurity and data privacy and protection are of concern.
- Recent high-profile cybersecurity events have drawn attention to the realities of how perpetrators can shut down operations, paralysing an entity's ability to deliver their core products and services.

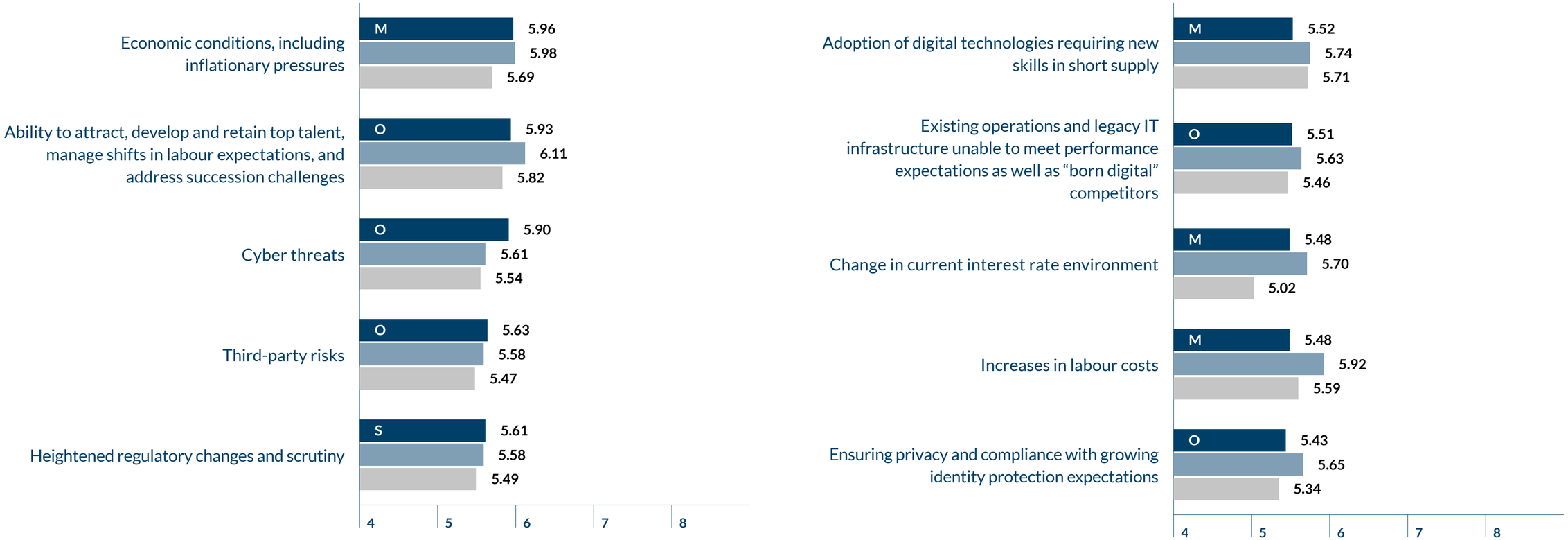
There is unease about existing operations and legacy IT systems limiting an organisation's ability to adjust core business processes to compete against more agile "born digital" competitors.

The one strategic risk issue in the 2024 top 10 risks relates to heightened regulatory changes and scrutiny.

The list of top 10 global risks for 2024, as noted by all survey participants, appears in Figure 2, along with their corresponding 2023 and 2022 scores (for those risks included in the prior years' surveys).

FIGURE 2

Top 10 risks for 2024



It is interesting that five of the top 10 risks are operational in nature, with four additional risks tied to macroeconomic concerns. Only one of the top 10 risks is of a strategic nature.

Consistent with the prior year study where only one of the top 10 risks was rated as a "Significant Impact" risk, none of the top 10 risks for 2024 is rated at that level. Three of the top 10 risks for 2024 are rated higher than they were in 2023: cyber threats, third-party risks, and heightened regulatory change and scrutiny.

Overarching concerns about economic conditions, particularly worries about ongoing inflationary pressures, are top of mind for executives for 2024. Uncertainties about policy decisions among central banks, coupled with concerns about the current interest rate environment (which also made the top 10 risks — ranked eighth — for 2024), may reflect executive worries about how the overall economy may restrict growth opportunities and squeeze margins as operating costs and the cost of capital are higher. Indeed, many executives must now operate in an environment of higher interest rates and inflation that they may have never faced before.

Macroeconomic challenges related to the labour market, particularly rising labour costs and difficulties in attracting unique skills needed to adopt emerging digital technologies successfully, add to economic concerns for global executives in 2024. Ongoing frustrations around compensation, managing flexible work options, mental health issues and other workplace challenges continue to create challenges in attracting and retaining the right talent needed for strategic success. Employee workplace expectations continue to evolve, union bargaining power is increasing and respondents are concerned that the organisation may not be able to adjust appropriately to compete in the highly competitive talent and skilled labour marketplace. This continues to create challenges for organisations as they attempt to determine their long-term strategies for talent acquisition and retention. Understandably, there are concerns about higher labour costs impacting profitability expectations.

Operational risks dominate the top 10 list of risks for 2024, with five of the top 10 risks linked to business process challenges. Technology-dependent operations, especially those related to ensuring appropriate cybersecurity and data privacy and protection, are of concern for executives, especially as expectations and regulations continue to increase surrounding the protection of systems and data. Recent high-profile cybersecurity events affecting name-brand entities, coupled with increased regulations in the United States surrounding disclosure requirements related to cyber events, have drawn attention to the realities of how perpetrators can shut down core operations,

Employee workplace expectations continue to evolve, union bargaining power is increasing and respondents are concerned that the organisation may not be able to adjust appropriately to compete in the highly competitive talent and skilled labour marketplace.

paralysing an entity's ability to deliver their core products and services until their demands, including ransomware payments, are met.

Concerns about existing operations and legacy IT systems limiting an organisation's ability to adjust core business processes to compete against more agile and nimble "born digital" competitors are adding to the overall operational risk profile on the minds of executives. To address these process limitations, many organisations are turning to third-party partners, joint ventures, and IT service providers and cloud computing to respond to evolving market conditions more quickly. While addressing process limitations and resilience objectives, the increased reliance on third parties is leading to a different risk concern regarding how risks and vulnerabilities at the third party may actually impact the organisations that are dependent on them. In light of that, concerns about third-party risks zoomed into the top 10 list of risks for 2024, jumping from the 17th position in 2023 to the fourth position for the coming year.

The one strategic risk in the 2024 top 10 risks relates to heightened executive concern about regulatory change and scrutiny affecting the way their organisation's processes are designed and products or services are produced or delivered. For example, recently approved climate-related risk disclosures for entities with operations in the European Union along with new and forthcoming climate-related disclosures for U.S. public entities, proliferating data privacy regulations, stronger focus on the timeliness and fairness of cyber breach disclosures, as well as industry-specific developments are significantly expanding expectations for aligning processes and emphasising disclosure enhancements on a timelier basis. In other situations, rising societal and market participant expectations, even outside those of a rulemaking nature, are raising the bar for how organisations can do business in the competitive marketplace, e.g., sustainability reporting and widespread greenwashing and greenhushing concerns. Meeting those expectations can be costly and impactful to reputation, brand image and profitability goals.

Majority of respondents view most top 10 risks as significant

Table 2 reveals the overall percentage of respondents who scored each of the top 10 risks at the "Significant Impact" (or "High) level (6.0 or higher), as well as the percentage of respondents who rate each as a 5.0 ("Medium") or as 4.0 or below ("Low") for 2024. This provides another perspective on the view of the top risk issues globally — the dispersion of the results distinct from individual average scores. The perception that the overall risk environment for 2024 continues to be significant (an average of 6.35 on a 10-point scale) is supported by the fact that 50% or more of board members and executives rate all of the top five risks at the "Significant Impact" level (e.g., they chose 6, 7, 8, 9 or 10 on our 10-point Likert scale), with just under a majority rating the remaining top 10 risks at the "Significant Impact" level. This disparity suggests uncertainty around the extent to which these top risks have the potential to impact most organisations noticeably in the coming year.

Many organisations are turning to third-party partners, joint ventures, and IT service providers and cloud computing to respond to evolving market conditions more quickly.

TABLE 2

Top 10 risks (with percentages of responses by impact level) — 2024[1]

Risk description	Type of risk	HIGH	MEDIUM	LOW
		6 -10	5	1-4
Economic conditions, including inflationary pressures	**Macroeconomic**	58%	16%	26%
Ability to attract, develop and retain top talent, manage shifts in labour expectations, and address succession challenges	**Operational**	56%	17%	27%
Cyber threats	**Operational**	56%	16%	28%
Third-party risks	**Operational**	53%	17%	30%
Heightened regulatory changes and scrutiny	**Strategic**	50%	17%	33%
Adoption of digital technologies requiring new skills in short supply	**Macroeconomic**	50%	16%	34%
Existing operations and legacy IT infrastructure unable to meet performance expectations as well as "born digital" competitors	**Operational**	50%	18%	32%
Change in current interest rate environment	**Macroeconomic**	49%	17%	34%
Increases in labour costs	**Macroeconomic**	49%	16%	35%
Ensuring privacy and compliance with growing identity protection expectations	**Operational**	48%	18%	34%

[1] The risks presented in Table 2 are in the same top 10 risk order as reported in Figure 2. That list is based on each risk's overall average score (using our 10-point scale). Table 2 merely reflects the percentage of respondents selecting a particular point (or range) on the 10-point scale.

Three-year comparison of risks

Each year, we provide an analysis of the overall three-year trends for the risks surveyed to provide insights about trending of individual risks. As discussed previously, to help identify differences in risk concerns across respondent type, we group all the risks based on their average scores into one of three classifications. Consistent with our prior studies, we use the following colour-coding scheme to highlight risks visually using these three categories.

Classification	Risks with an average score of	
Significant Impact	**6.0 or higher**	●
Potential Impact	**4.51 through 5.99**	●
Less Significant Impact	**4.5 or lower**	●

In Table 3, we summarise the impact assessments for each of the 36 risks for the full sample arranged by the three categories of risks we analyse: macroeconomic, strategic and operational. For each risk, the column labelled "2024 Rank" indicates that risk's relative position among the 36 risks for 2024, with rank "1" representing the risk with the highest overall impact score for 2024.

Even though a majority of respondents rated all of the top five risks at the "Significant Impact" level, none of the 36 risks is, on average, at the "Significant Impact" level when combining the ratings of all respondents for each risk. This is relatively consistent with the prior three years, where one in 2023, none in 2022 and only one in 2021 were rated at that level, even during the COVID-19 pandemic. The other 35 risk issues fall into the category of "Potential Impact" risks. None of the risks is rated at the lowest level ("Less Significant Impact") for 2024, which is consistent with last year. This suggests that all of the 36 risks examined in this study represent highly relevant concerns to be considered by board members and executives.

"The shift in what comprises the top risk concerns for 2024 from prior years highlights the reality that conditions are constantly evolving, with new uncertainties unfolding on a continual basis. This calls for risk management processes that are nimble and ongoing and that focus on the speed at which different risks may evolve. Mere periodic risk management is insufficient in today's rapidly changing environment."

MARK BEASLEY
PROFESSOR OF ENTERPRISE RISK MANAGEMENT, POOLE COLLEGE OF MANAGEMENT, NC STATE UNIVERSITY

TABLE 3

Perceived impact for 2024 relative to prior years — full sample

Macroeconomic Risk Issues	2024 Rank	2024	2023	2022
Economic conditions, including inflationary pressures	1	●	●	●
Adoption of digital technologies requiring new skills in short supply	6	●	●	●
Change in current interest rate environment	8	●	●	●
Increases in labour costs	9	●	●	●
Geopolitical shifts, regional conflicts and instability in governmental regimes or expansion of global terrorism	20	●	●	●
Volatility in global financial markets and currency exchange rates	23	●	●	●
Impact of social issues and DEI priorities on ability to attract/retain talent and compete	27	●	●	●
Access to capital/liquidity	30	●	●	●
Changes in global markets and trade policies	34	●	●	●
Pandemic-related government policies and regulation	36	●	●	●

Strategic Risk Issues	2024 Rank	2024	2023	2022
Heightened regulatory changes and scrutiny	5	●	●	●
Sustaining customer loyalty and retention	12	●	●	●
Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces	13	●	●	●
Organisation not sufficiently resilient and/or agile to manage an unexpected crisis	16	●	●	●
Limited opportunities for organic growth	18	●	●	●
Growing focus on climate change and other sustainability policies, regulations, and expanding disclosure requirements as well as expectations of key stakeholders	22	●	●	●
Social media developments and platform technology innovations	25	●	●	●
Ease of entrance of new competitors or other changes in competitive environment	26	●	●	●
Substitute products and services that affect the viability of our business	28	●	●	●
Difficulty in growing through acquisitions, joint ventures and other activities	31	●	●	●
Formulating business response to legal, political and social issues that are polarising	33	●	N/A	N/A
Performance shortfalls that trigger activist shareholders	35	●	●	●

Operational Risk Issues	2024 Rank	2024	2023	2022
Ability to attract, develop and retain top talent, manage shifts in labour expectations, and address succession challenges	2	●	●	●
Cyber threats	3	●	●	●
Third-party risks	4	●	●	●
Existing operations and legacy IT infrastructure unable to meet performance expectations as well as "born digital" competitors	7	●	●	●
Ensuring privacy and compliance with growing identity protection expectations	10	●	●	●
Inability to utilise rigorous data analytics to achieve market intelligence and increase productivity and efficiency	11	●	●	●
Resistance to change restricting organisation from adjusting business model and core operations	14	●	●	●
Challenges in sustaining culture due to changes in overall work environment	15	●	●	●
Organisation's culture not sufficiently encouraging timely identification and escalation of emerging risk issues	17	●	●	●
Uncertainty surrounding core supply chain ecosystem	19	●	●	●
Rising threat of catastrophic natural disasters and weather phenomena	21	●	●	N/A
Managing demands on or expectations of workforce to work remotely or as part of a hybrid work environment	24	●	●	●
Enhanced exposure to fraud in the industry	29	●	N/A	N/A
Meeting expectations around protecting health and safety of employees (including their well-being and mental health), customers, suppliers and our communities	32	●	●	●

Risks with largest increase from prior year

To highlight the most dramatic shifts in year-over-year perceptions, we also investigate which risks increased the most from 2023 to 2024. Only three of the 34 risks[2] that we surveyed in the prior year have average overall scores that are higher than the average scores in 2023. The 31 remaining risks decreased from 2023. In Table 4, we show the five risks that increased the most (or decreased the least) from 2023.

TABLE 4

The five risks with highest level of increase (or smallest decrease) — 2024 vs. 2023

Risk description	2024	2023	Percentage change
Cyber threats	5.90	5.61	5.27%
Third-party risks	5.63	5.58	0.87%
Heightened regulatory changes and scrutiny	5.61	5.58	0.51%
Economic conditions, including inflationary pressures	5.96	5.98	-0.38%
Existing operations and legacy IT infrastructure unable to meet performance expectations as well as "born digital" competitors	5.51	5.63	-2.16%

The two highest increasing risks for 2024 over 2023 are both operational risks related to cyber threats and third-party issues. The third risk that increased over the prior year is the strategic risk related to concerns about heightened regulatory change and scrutiny affecting the way products or services can be delivered to the market.

[2] Recall that two new risks were added to this year's survey.

Risks with largest decrease from prior year

Thirty-one risks decreased in severity in 2024 from 2023. The five risks that exhibited the largest percentage decrease are highlighted in Table 5.

TABLE 5

The five risks with highest level of decrease — 2024 vs. 2023

Risk description	2024	2023	Percentage change
Pandemic-related government policies and regulation	4.62	5.54	-16.57%
Performance shortfalls that trigger activist shareholders	4.64	5.34	-13.15%
Managing demands on or expectations of workforce to work remotely or as part of a hybrid work environment	4.97	5.71	-12.93%
Uncertainty surrounding core supply chain ecosystem	5.04	5.79	-12.87%
Difficulty in growing through acquisitions, joint ventures and other activities	4.87	5.52	-11.78%

Three of the risks in Table 5 reflect concerns triggered by conditions tied to the pandemic. The decline regarding government policies and regulation suggests that respondents view COVID-19 as endemic in nature. The other two pandemic-related risks — managing expectations of the workforce and uncertainty surrounding supply chain issues — have subsided as the market has evolved and adjusted. Additionally, concerns related to M&A activities and to activist shareholders seem to be somewhat diminished for 2024 relative to 2023.

Longer-term perspective — overview of risks for 2034

What you need to know

A riskier long-term outlook: Executives rate nine of the top 10 risks for 2034 higher than they rated the same risks last year as they looked a decade out.

Cyber threats are the top long-term risk issue, with a sizeable year-over-year increase in risk score.

Innovation and technology concerns dominate the top five risks for 2034. Executives are focused on whether their organisations can respond to rapidly emerging innovations that may disrupt their business models and operations.

Talent risks also stand out: Lack of ability to attract, develop and retain the talent needed to manage emerging technologies may significantly impede competitive capabilities in the marketplace.

- Those concerns reflect an overall worry about the ability to compete in the marketplace profitably in the long term.

Eyeing the regulatory landscape: Executives and boards are focused on the potential for new regulations to emerge — related to social, privacy and environmental issues, among other changes — as expectations around what is deemed acceptable continue to shift.

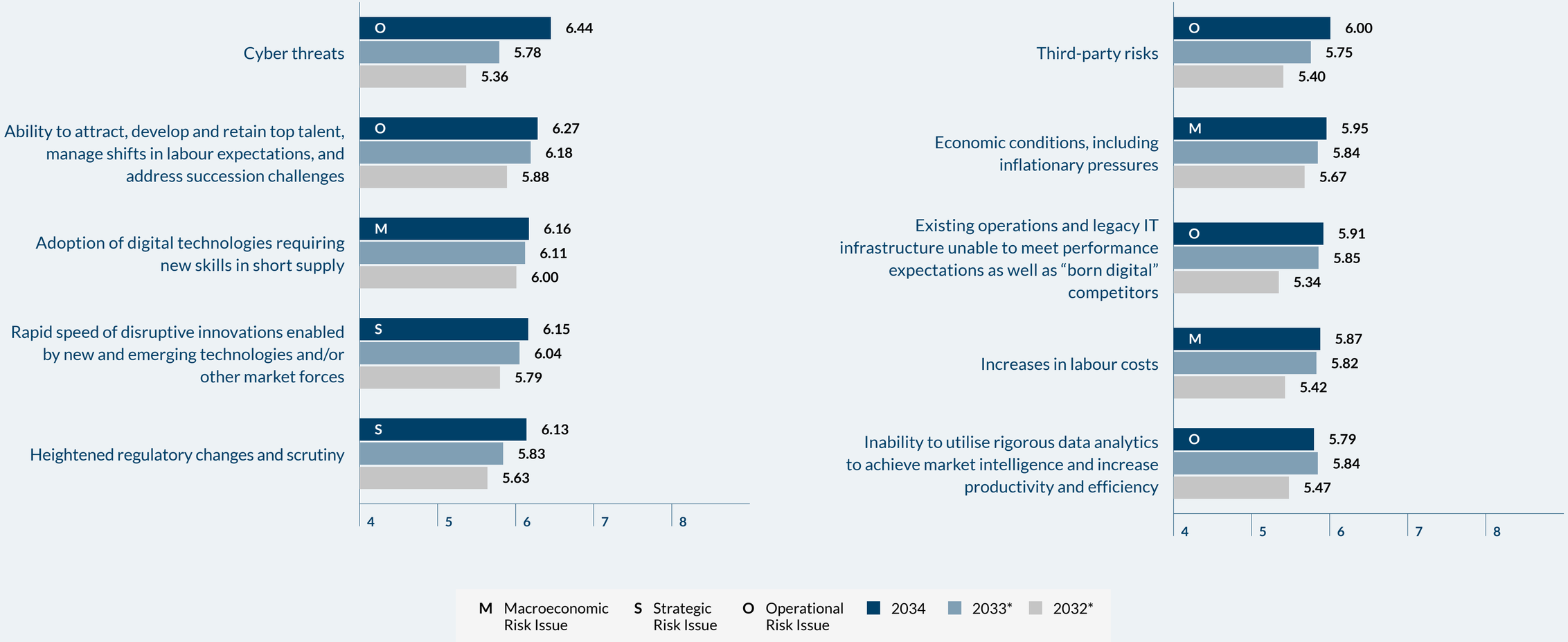
The interrelated nature of global risks: Despite efforts to retreat from globalisation, organisations continue to operate in an interdependent but highly competitive global marketplace. Shifting global optics create fresh nuances and complexities in evaluating global risks.

Between the lines: There is significant overlap in the risk landscape when comparing the top 10 short-term risks (2024) with the long-term risks (2034). This continuity suggests short-term risk concerns may have a lingering impact on organisations over the next decade.

In addition to obtaining respondent perspectives about risks on the horizon for 2024, we asked them to provide insights about long-term impacts of those same risks over the next decade — 2034. The top 10 global risks for 2034 appear in Figure 3, alongside scores from our two prior years (also looking out a decade ahead when asked).

FIGURE 3

Top 10 risks for 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.

What is striking about the long-term view of risks is that executives rate nine of the top 10 risks for 2034 higher than they rated the same risks last year as they looked a decade out. This suggests that concerns about long-term risks are greater than what they perceived last year. This is especially noticeable when viewing the sizeable increase in the perceived risk of cyber threats for 2034, which is the number one risk concern a decade out.

Innovation, technology and related talent concerns dominate the top five risks for 2034. In addition to cyber threats making the top of the risk list, executives are also focused on whether their organisations will be able to respond to rapidly emerging innovations that can disrupt business models and the way they do business. Their lack of ability to attract, develop and retain the talent needed to manage emerging technologies may significantly impede their competitive capabilities in the marketplace. Those concerns, coupled with potential limitations tied to existing operations and legacy IT systems and increases in labour costs to retain the talent once acquired, reflect an overall worry about their abilities to compete in the marketplace profitably in the long term. Limited digital thinking and expertise, particularly in the C-suite, may make it difficult for the organisation to compete in a digital marketplace. Furthermore, survey respondents are concerned about having the data analytics and "big data" capabilities to gain insights about customer experiences and markets to inform decision-making as well as take advantage of operational efficiency opportunities. Clearly, talent and technology concerns are intertwined over the long term.

Risks related to the escalation of regulatory changes and scrutiny, worries about growing dependencies on third-party relationships to do business, and long-lasting unfavourable economic conditions dominate the list of risk concerns for executives as they look into long-term horizons. Respondents are also focused on potential shifts in regulatory priorities and how changes in regulations might impact the way their organisations' processes are designed and how their products are produced and delivered. As executives and boards look a decade out, they are focused on the potential for new regulations to emerge as expectations around what is deemed acceptable continue to shift. Perhaps, as these leaders reflect on rapidly shifting expectations over the last decade — or even recent years — related to social, privacy and environmental issues, among other changes, they are projecting ahead a similar noticeable shift as they keep a wary eye on potential scenarios and developments over the next decade.

But there is another important dimension to the long-term outlook — the running thread through this survey report regarding the interrelated nature of global risks. As noted in our commentary regarding the post-October 7 survey results, the attack on Israel resulted in an uptick in the risks rated after the war started. Despite efforts to retreat from globalisation, the reality is that organisations continue to operate in an interdependent but highly competitive global marketplace. Shifting global optics create fresh nuances and complexities in evaluating global risks.

There is quite a bit of overlap in the risk landscape when comparing the top 10 short-term risks (2024) with the long-term risks (2034). Eight of the top 10 risks appear on both lists. Likewise, eight of the top 10 risks looking out 10 years last year are on this year's list. This continuity suggests that the short-term risk concerns noted this year may likely have a lingering impact on organisations over the next decade.

Table 6 highlights the two risks making the top 10 for 2034 that were not in the top 10 for 2024. Strategic concerns related to the rapid speed of disruptive innovations enabled by new and emerging technologies (e.g., generative AI) and other market forces suggest executives are focused on ensuring their organisations can compete successfully by changing at the speed of the market. Respondents are also concerned about their organisation's inability to utilise rigorous data analytics to achieve market intelligence, connect with the customer experience, and identify operational and market efficiencies.

TABLE 6

Two risks for 2034 not in top 10 list for 2024

Risk description	2034 Rank	2034 Response	2024 Rank	2024 Response
Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces	4	6.15	13	5.28
Inability to utilise rigorous data analytics to achieve market intelligence and increase productivity and efficiency	10	5.79	11	5.42

Recall that risks with average scores of 6.0 or higher are classified as "Significant Impact" risks, while risks with average scores of 4.51 through 5.99 are classified as having a "Potential Impact." Risks with average scores 4.5 or below are classified as having a "Less Significant Impact." In Figure 3, we see that six of the top 10 long-term risks are rated at the "Significant Impact" level looking out to 2034. This is in contrast to three of the top 10 risks rated at that level looking out 10 years last year and only one of the top 10 long-term risks rated at that level the year before. These differences suggest heightened uncertainty a decade out relative to short-term concerns.

Table 7 presents the percentage of respondents who rate the top 10 risks into one of these three classifications. A majority of respondents rate all of the top 10 risks at the "Significant Impact" level for 2034. The fact that all are rated at the higher level for a decade out suggests respondents are especially concerned as they look at long-term horizons.

A majority of respondents rate all of the top 10 risks at the "Significant Impact" level for 2034.

TABLE 7

Top 10 risks (with percentages of responses by impact level) — 2034[3]

Risk description	Type of risk	HIGH	MEDIUM	LOW
		6 -10	5	1-4
Cyber threats	**Operational**	65%	15%	20%
Ability to attract, develop and retain top talent, manage shifts in labour expectations, and address succession challenges	**Operational**	61%	17%	22%
Adoption of digital technologies requiring new skills in short supply	**Macroeconomic**	60%	17%	23%
Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces	**Strategic**	58%	17%	25%
Heightened regulatory changes and scrutiny	**Strategic**	60%	16%	24%
Third-party risks	**Operational**	58%	18%	24%
Economic conditions, including inflationary pressures	**Macroeconomic**	55%	20%	25%
Existing operations and legacy IT infrastructure unable to meet performance expectations as well as "born digital" competitors	**Operational**	54%	18%	28%
Increases in labour costs	**Macroeconomic**	54%	20%	26%
Inability to utilise rigorous data analytics to achieve market intelligence and increase productivity and efficiency	**Operational**	50%	21%	29%

[3] The risks presented in Table 7 are in the same top 10 risk order as reported in Figure 3. That list is based on each risk's overall average score (using our 10-point scale). Table 7 merely reflects the percentage of respondents selecting a particular point (or range) on the 10-point scale.

Table 8 shows the risks with the biggest differences between the 2024 and 2034 scores, with all of them reflecting increases in risk scores from 2024 to 2034. Interestingly, four of the five risks with the biggest differences in short-term versus long-term views (e.g., 2024 versus 2034 average risk scores) represent strategic risk issues. Concerns related to disruptive innovations and emerging technologies, concerns that some innovations may lead to substitute products and services, and concerns about lower barriers for new market entrants make up the top three biggest increasing risks over the next decade. Risks related to the growing focus on climate change and other sustainability policies and regulations and the availability of skills needed to adopt emerging digital technologies are especially heightened for executives as they look out a decade.

TABLE 8

Five risks with largest positive differences between 2024 and 2034

Risk description	2024	2034	Percentage change
Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces *(strategic)*	5.28	6.15	16.40%
Substitute products and services that affect the viability of our business *(strategic)*	4.89	5.58	14.14%
Ease of entrance of new competitors or other changes in competitive environment *(strategic)*	4.91	5.59	13.91%
Growing focus on climate change and other sustainability policies, regulations, and expanding disclosure requirements as well as expectations of key stakeholders *(strategic)*	5.01	5.70	13.67%
Adoption of digital technologies requiring new skills in short supply *(macroeconomic)*	5.52	6.16	11.63%

Table 9 shows the average risk score for 2034 for each of the 36 risks included in our survey organised by risk category: macroeconomic, strategic and operational. Six of the risks are at the "Significant Impact" level as executives think about 2034. All other risks are at the "Potential Impact" level. None are at the "Less Significant Impact" level.

TABLE 9

Perceived impact for 2034 relative to prior years — full sample

Macroeconomic Risk Issues	2034 Rank	2034	2033*	2032*
Adoption of digital technologies requiring new skills in short supply	3	●	●	●
Economic conditions, including inflationary pressures	7	●	●	●
Increases in labour costs	9	●	●	●
Change in current interest rate environment	19	●	●	●
Geopolitical shifts, regional conflicts and instability in governmental regimes or expansion of global terrorism	23	●	●	●
Volatility in global financial markets and currency exchange rates	26	●	●	●
Changes in global markets and trade policies	28	●	●	●
Impact of social issues and DEI priorities on ability to attract/retain talent and compete	30	●	●	●
Access to capital/liquidity	34	●	●	●
Pandemic-related government policies and regulation	36	●	●	●

* 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.

Strategic Risk Issues	2034 Rank	2034	2033*	2032*
Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces	4			
Heightened regulatory changes and scrutiny	5			
Sustaining customer loyalty and retention	12			
Growing focus on climate change and other sustainability policies, regulations, and expanding disclosure requirements as well as expectations of key stakeholders	13			
Ease of entrance of new competitors or other changes in competitive environment	16			
Substitute products and services that affect the viability of our business	17			
Limited opportunities for organic growth	20			
Organisation not sufficiently resilient and/or agile to manage an unexpected crisis	22			
Social media developments and platform technology innovations	24			
Difficulty in growing through acquisitions, joint ventures and other activities	27			
Formulating business response to legal, political and social issues that are polarising	29		N/A	N/A
Performance shortfalls that trigger activist shareholders	32			

* 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.

Operational Risk Issues	2034 Rank	2034	2033*	2032*
Cyber threats	1	●	●	●
Ability to attract, develop and retain top talent, manage shifts in labour expectations, and address succession challenges	2	●	●	●
Third-party risks	6	●	●	●
Existing operations and legacy IT infrastructure unable to meet performance expectations as well as "born digital" competitors	8	●	●	●
Inability to utilise rigorous data analytics to achieve market intelligence and increase productivity and efficiency	10	●	●	●
Ensuring privacy and compliance with growing identity protection expectations	11	●	●	●
Challenges in sustaining culture due to changes in overall work environment	14	●	●	●
Rising threat of catastrophic natural disasters and weather phenomena	15	●	●	N/A
Resistance to change restricting organisation from adjusting business model and core operations	18	●	●	●
Organisation's culture not sufficiently encouraging timely identification and escalation of emerging risk issues	21	●	●	●
Uncertainty surrounding core supply chain ecosystem	25	●	●	●
Enhanced exposure to fraud in the industry	31	●	N/A	N/A
Managing demands on or expectations of workforce to work remotely or as part of a hybrid work environment	33	●	●	●
Meeting expectations around protecting health and safety of employees (including their well-being and mental health), customers, suppliers and our communities	35	●	●	●

* 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.

Analysis across different sizes of organisations

What you need to know

Important takeaway: Organisations of all sizes perceive a slight decrease in the magnitude and severity of risks in 2024 for their organisations in comparison to 2023, but their overall assessments of magnitude and severity of risks are higher than two years earlier.

What is striking for 2024 is the general higher level of risk concerns for the two categories of smaller organisations, which rate all of their top five risks as higher in 2024 relative to 2023.

- In contrast, none of the top five risks for the largest organisations are at the "Significant Impact" level, suggesting smaller-sized organisations perceive the risk environment as more impactful for them in 2024 relative to larger organisations.

Three risks are common top five risks across all size groups:

1. Attracting and retaining talent, including succession challenges
2. Economic conditions and inflationary pressures
3. Cyber threats

Heightened regulatory change and scrutiny is a top five risk for the two largest size categories of organisations.

For the 2034 risk outlook, the differences in perceptions relative to near-term risk concerns for 2024 is striking. Across all sizes of organisations, respondents rate their top five long-term risks at higher levels than their 2024 outlooks.

- In each of the four size categories, respondents rate all top five risks at "Significant Impact" levels.
- Leaders must think in terms of multiple scenarios and how they may play out over time. While this thinking facilitates preparedness and a more robust strategic outlook, it also highlights their uncertainty in facing the future.

The bottom line: Notable long-term risks include cyber threats; adoption of emerging digital technologies; attracting, developing and retaining talent; and heightened regulatory changes and scrutiny.

The sizes of organisations, as measured by total organisational revenue, vary across our 1,143 respondents, as shown in the accompanying table.

The mix of sizes of organisations represented by respondents is very similar to the mix of respondents in our prior years' surveys. About 63% of our respondents are in larger organisations with revenues between $1B or higher.

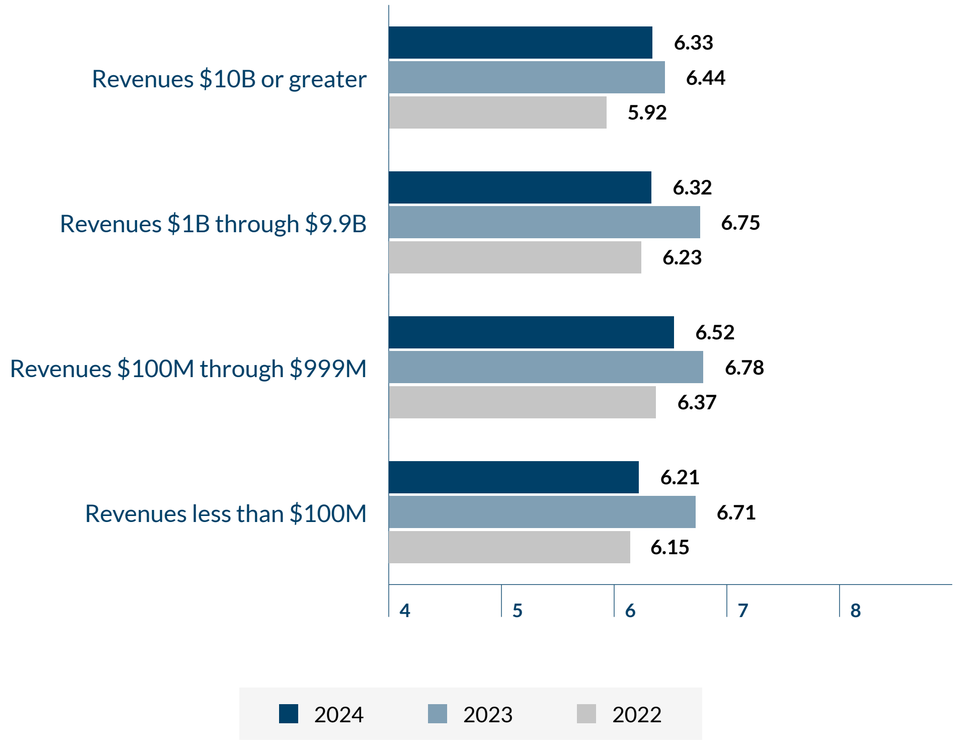
Most recent fiscal year revenues	Number of respondents
Revenues $10 billion or greater	256
Revenues $1 billion to $9.99 billion	461
Revenues $100 million to $999 million	265
Revenues less than $100 million	161
Total number of respondents	**1,143**

The overall outlook about risk conditions differs across sizes of organisations. We asked respondents to provide their overall impression of the magnitude and severity of risks their organisation will be facing using a 10-point scale where 1 = "Extremely Low" and 10 = "Extremely High."

Organisations of all sizes perceive a slight decrease in the magnitude and severity of risks in 2024 for their organisations in comparison to 2023, but their overall assessments of magnitude and severity of risks are higher than two years earlier. This suggests some general improvement in risk conditions year-over-year, but caution still remains. In addition, all organisations indicate that the magnitude and severity of risks will be greater than 6.0 and have a significant impact over the next 12 months. Organisations with revenues between $100 million and $999 million perceive their overall business environment to be riskier relative to all other sizes of organisations, with an impact score of 6.52.

FIGURE 4

Overall, what is your impression of the magnitude and severity of risks your organisation will be facing with respect to achieving your performance goals over the next 12 months?



2024 risk issues

What is striking for 2024 is the general higher level of risk concerns for the two categories of smaller organisations (those with revenues below $1 billion). In both categories, respondents rated all of their top five risks as higher in 2024 relative to 2023. Two of the top five risks are at the "Significant Impact" level for organisations with revenues between $100 million and $999 million, while three of the top five risks for organisations with revenues less than $100 million are at that level. In contrast, none of the top five risks for the largest organisations (revenues greater than $10 billion) is at the "Significant Impact" level, and none of the top five risks for organisations with revenues between $1 billion and $9.9 billion is rated at that level. Collectively, this suggests smaller-sized organisations perceive the risk environment as more impactful for them in 2024 relative to larger organisations.

Three risks are common top five issues across all size groups: (1) Concerns about attracting and retaining talent, including succession challenges; (2) concerns that economic conditions (and inflationary pressures) in markets served may affect growth and profitability; and (3) concerns about cyber threats. Except for the largest size organisations, concerns about economic conditions represent the first- or second-ranked risk across all organisation sizes, while cybersecurity concerns are higher in the top five list of risks for the two largest-sized organisation categories relative to the smaller categories. Perhaps their sizes may be perceived as increasing their visibility to cyber threat perpetrators who might seek to target more recognisable companies and brands in the marketplace.

Concerns about heightened regulatory changes and scrutiny are a top five risk for the two largest-size categories of organisations. Some of these regulations, such as the new climate-related disclosure rules in the European Union (and the SEC's proposed climate disclosure rules) and other matters discussed earlier, come with expanded responsibilities for the largest organisations. The largest organisations are also especially concerned about risks related to their existing operations and legacy IT systems. That risk was not in the top five list of risks for all other sizes of organisations.

Third-party risks make the list of top five risk concerns for organisations in the two middle ranges of organisational size. Perhaps reliance on third-party partners and vendors is more notable for these organisations as they seek growth opportunities over time. The two smaller-sized categories of organisations rate in their top five lists risks tied to a perceived lack of skills needed for their adoption of digital technologies. Smaller organisations may face greater hurdles in embracing emerging innovation as they compete for talent to help them leverage the advantages and value proposition offered by new technological advancements.

Smaller organisations may face greater hurdles in embracing emerging innovation as they compete for talent to help them leverage the advantages and value proposition offered by new technological advancements.

2034 risk issues

The differences in perceptions about long-term risk conditions relative to near-term risk concerns for 2024 are striking. Across all sizes of organisations, respondents rate their top five long-term risks at higher levels than their 2024 outlooks. In each of the four size categories, respondents rate all top five risks at "Significant Impact" levels, suggesting that their concerns about 2034 are at a higher risk level relative to their near-term risk concerns. Additionally, the two smaller size categories of organisations rate all of their top five risks higher than their assessments of long-term risks in last year's study. Clearly, respondents are expressing greater pause about long-term outlooks this year relative to those outlooks last year. This is not surprising. In an era of disruptive change, leaders must think in terms of multiple scenarios and how they may play out over time. While this thinking facilitates preparedness and a more robust strategic outlook among organisations, it also highlights their uncertainty in facing the future, often escalating perceptions of strategic and macroeconomic risks and, interestingly, even operational risks such as cyber threats and talent challenges.

Technology-themed concerns dominate the list of top risks for a decade from now. All sizes of organisations rate cyber threats as a top five risk, with all except the very largest size category rating that concern as their number one risk issue. Concerns about the ability to adopt emerging digital technologies also is in the top five risks for all organisations, and risks related to the rapid speed of disruptive innovations enabled by new and emerging technologies made the top five risks for all sizes of organisations, except the smallest size category.

Talent concerns also remain a top risk for all sizes of organisations, as each category includes concerns related to their ability to attract, develop and retain talent, including succession challenges, as a top five risk. Uncertainty about heightened regulatory changes and scrutiny is top of mind for the two largest size categories of organisations, especially for the largest organisations (revenues of $10 billion or higher), which rank that concern as their top risk issue for 2034. Only the smallest organisations highlight concerns about privacy and data security and concerns about economic conditions as top five long-term risk challenges.

Figures 5-8 summarise the top-rated risks by size of organisation separately for 2024 and 2034. Only the top five risks are reported for each year, along with prior year risk scores.

Technology-themed concerns dominate the list of top risks for a decade from now.

FIGURE 5A

Revenues $10B or greater — 2024

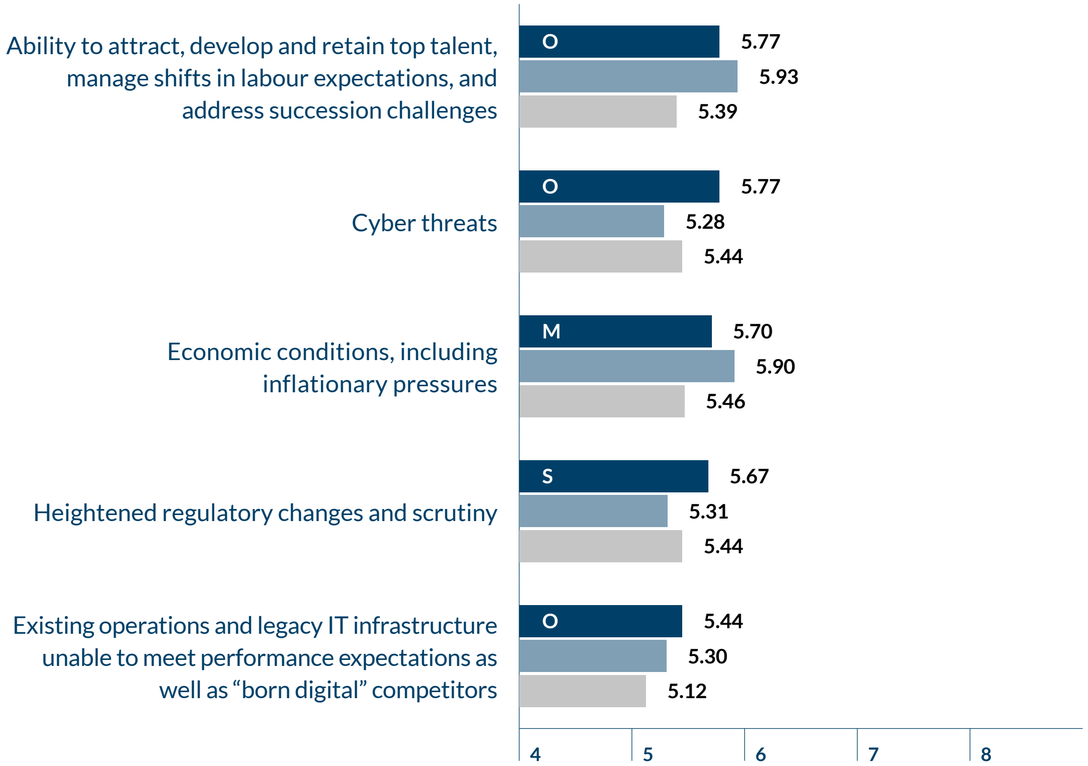
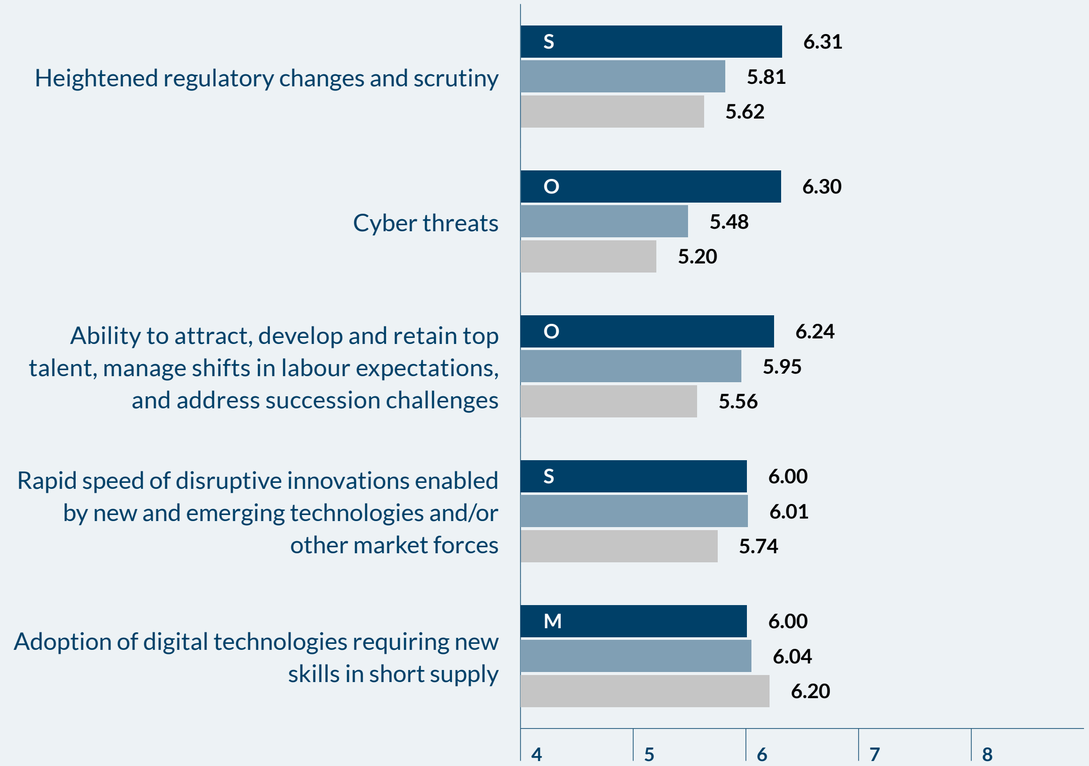


FIGURE 5B

Revenues $10B or greater — 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.

FIGURE 6A

Revenues $1B - $9.99B — 2024

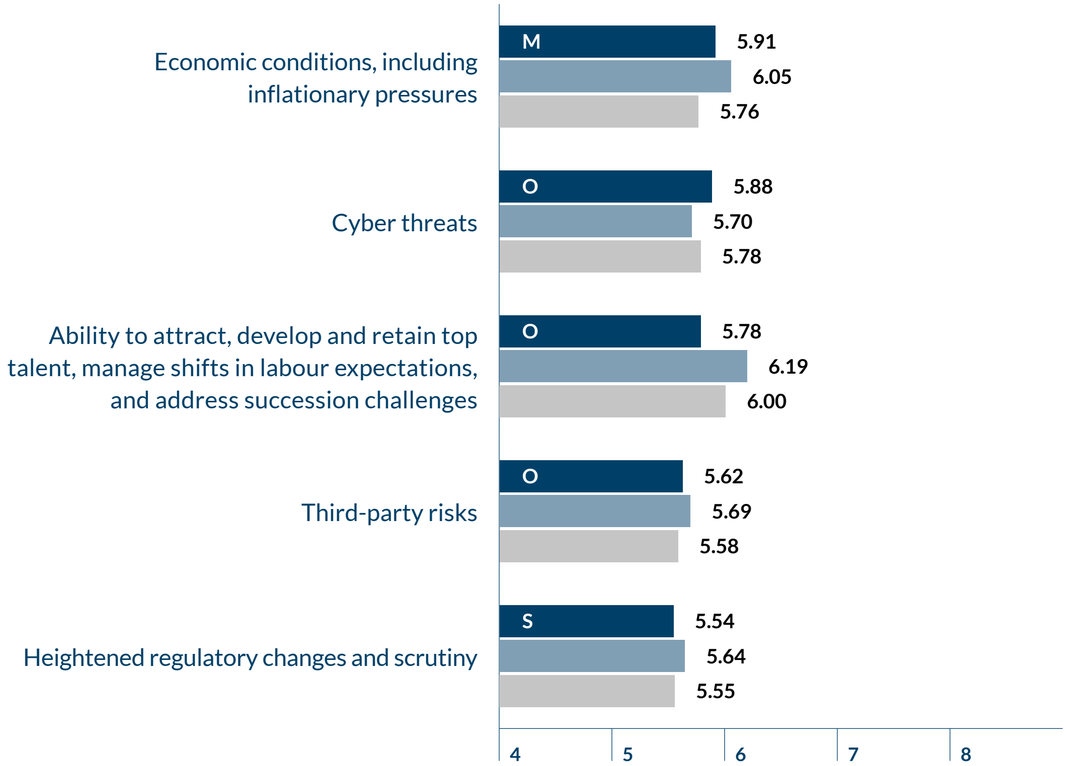
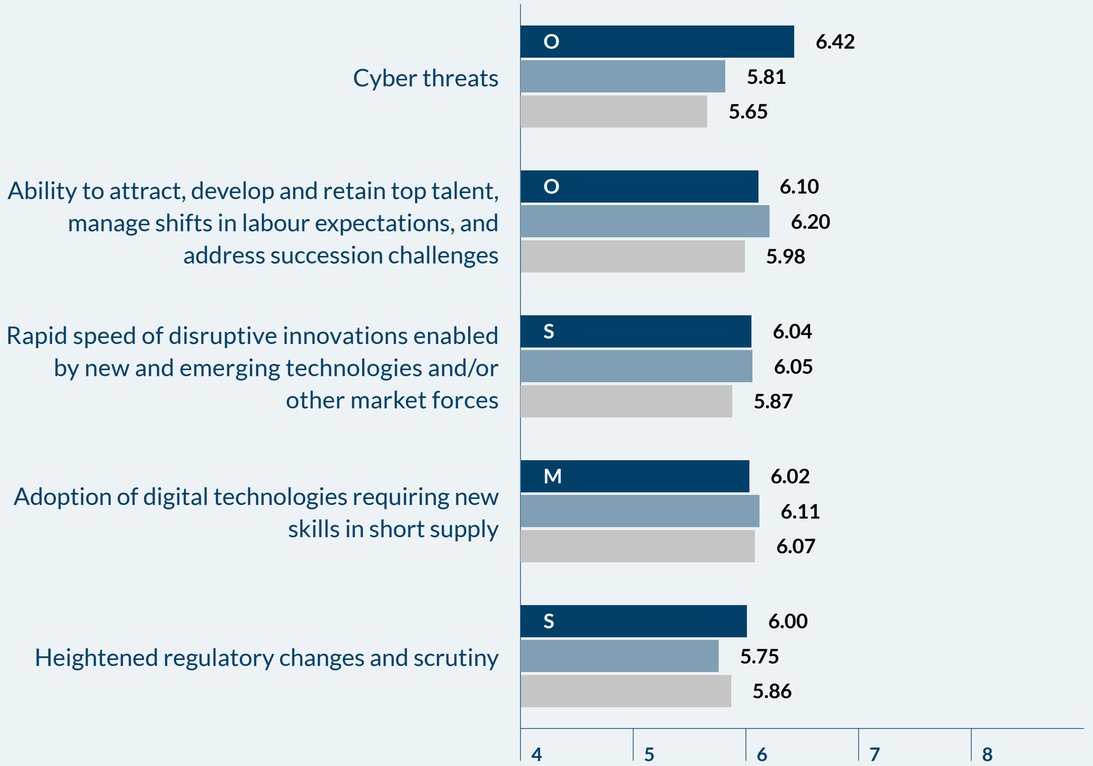


FIGURE 6B

Revenues $1B - $9.99B — 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.

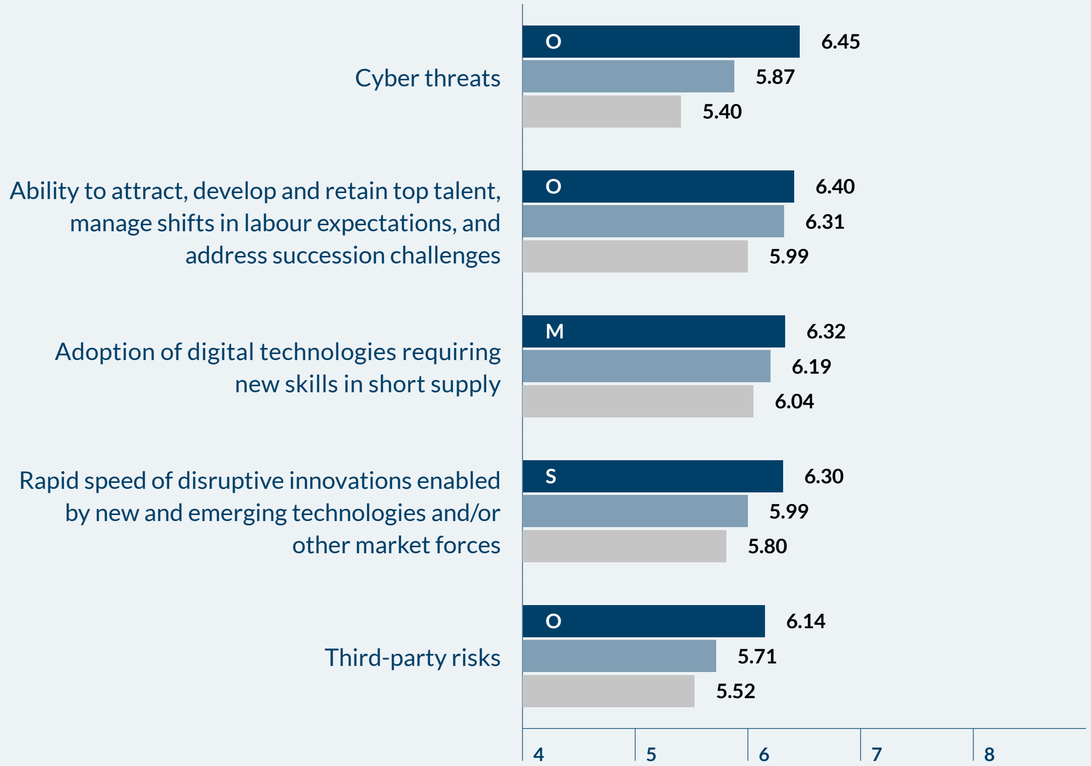
FIGURE 7A

Revenues $100M - $999M — 2024

M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue 2024 2023 2022

FIGURE 7B

Revenues $100M - $999M — 2034



M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue 2034 2033* 2032*

* 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.

FIGURE 8A

Revenues less than $100M — 2024

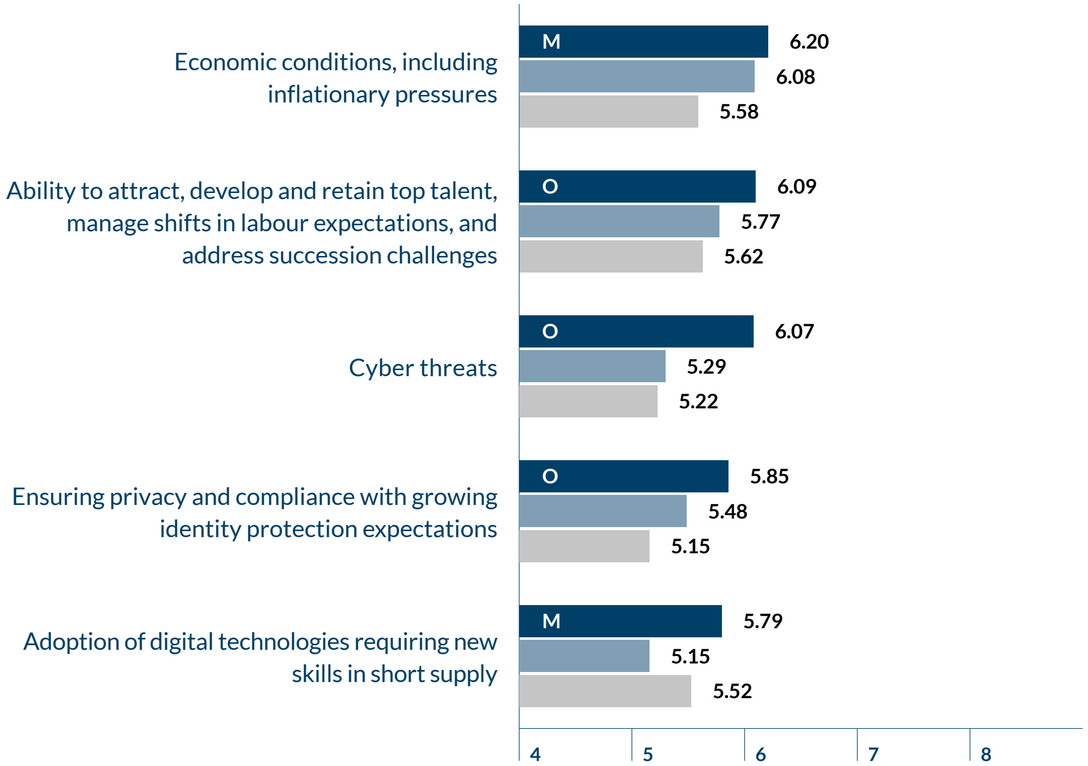
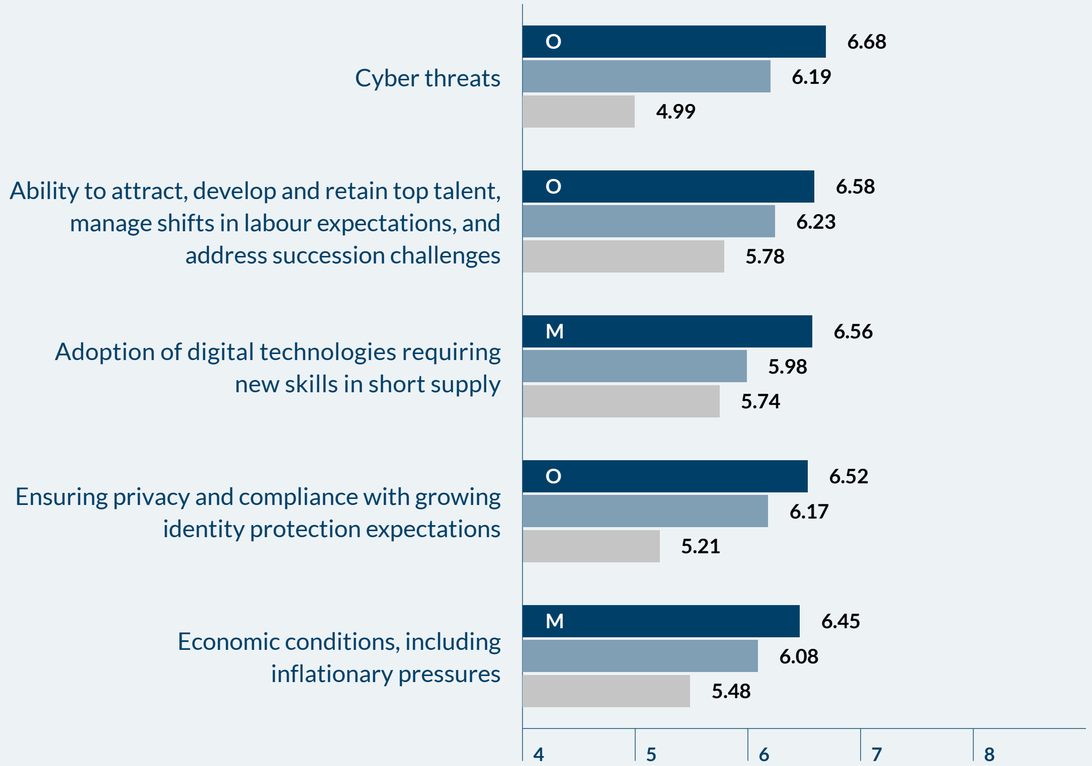


FIGURE 8B

Revenues less than $100M — 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.

Analysis across executive positions represented

What you need to know

The big picture: Overall impressions across executive positions with respect to the magnitude and severity of risks in the environment are that the level of risk looking forward to 2024 has decreased in comparison to last year's outlook for 2023.

- In relation to our prior year results, almost every group of executives reduced the number of risks they rated as "Significant Impact."
- Most positions identify attracting and developing talent and economic conditions as top five risks.
- There is variation in perspectives across different executive positions, which calls for more discussion among executive members to better understand how each group views the risk landscape and obtain a clearer view of the organisation's risk profile.

The next decade: Looking to 2034, overall risk perceptions exhibit significant variation relative to 2024.

- Board members rate three of their top five risk issues at the "Significant Impact" level.
- CAEs have the most concern about the future, rating 15 risks at the "Significant Impact" level.
- The 2034 results show an increase in overall risk concerns for 2034 relative to short-term risk concerns for 2024.

Key takeaway: The results reflect how different roles offer varying perspectives when assessing risks in disparate environments and over longer versus shorter time horizons.

Gathering diverse perspectives: The results illustrate the importance of bringing varying perspectives to the ERM process.

- Each executive needs to identify and assess risks in disparate environments and over longer versus shorter time horizons.
- The board and management team should engage in dialogue regarding the most critical enterprise risks, given the different perspectives each brings to the table.
- Without clarity of focus, the executive team may not be aligned both internally and with the board on what the top risks are. Worse, they may not be appropriately addressing the most important risks the organisation faces.

We targeted our survey to individuals currently serving on the board of directors or in senior executive positions so that we could capture board and C-suite perspectives about risks on the horizon for 2024 and a decade later (2034). We received responses from 109 members of a board of directors, and it is reasonable to expect that some C-suite executives also serve on one or more boards. An additional 100 respondents serve as CEOs for their organisations. As indicated in the accompanying table, 87 responses were received from individuals who did not fit within one of our executive categories. Their responses are included in the full sample of 1,143 but are not separately analysed.

Executive position	Number of respondents
Board Member (Board)	109
Chief Executive Officer (CEO)	100
Chief Financial Officer (CFO)	105
Chief Human Resources Officer (CHRO)	42
Chief Risk Officer (CRO)	180
Chief Audit Executive (CAE)	193
Chief Information/Technology Officer (CIO/CTO)	131
Chief Strategy/Innovation Officer (CSO)	51
Chief Data/Digital Officer (CDO)	48
Other C-Suite[4] (OCS)	97
All Other[5]	87
Total number of respondents	**1,143**

[4] This category includes titles such as chief operating officer, general counsel and chief compliance officer.

[5] These 87 individuals either did not provide a response allowing for classification by position or would best be described as middle management or business advisers/consultants. We do not provide a separate analysis for this category.

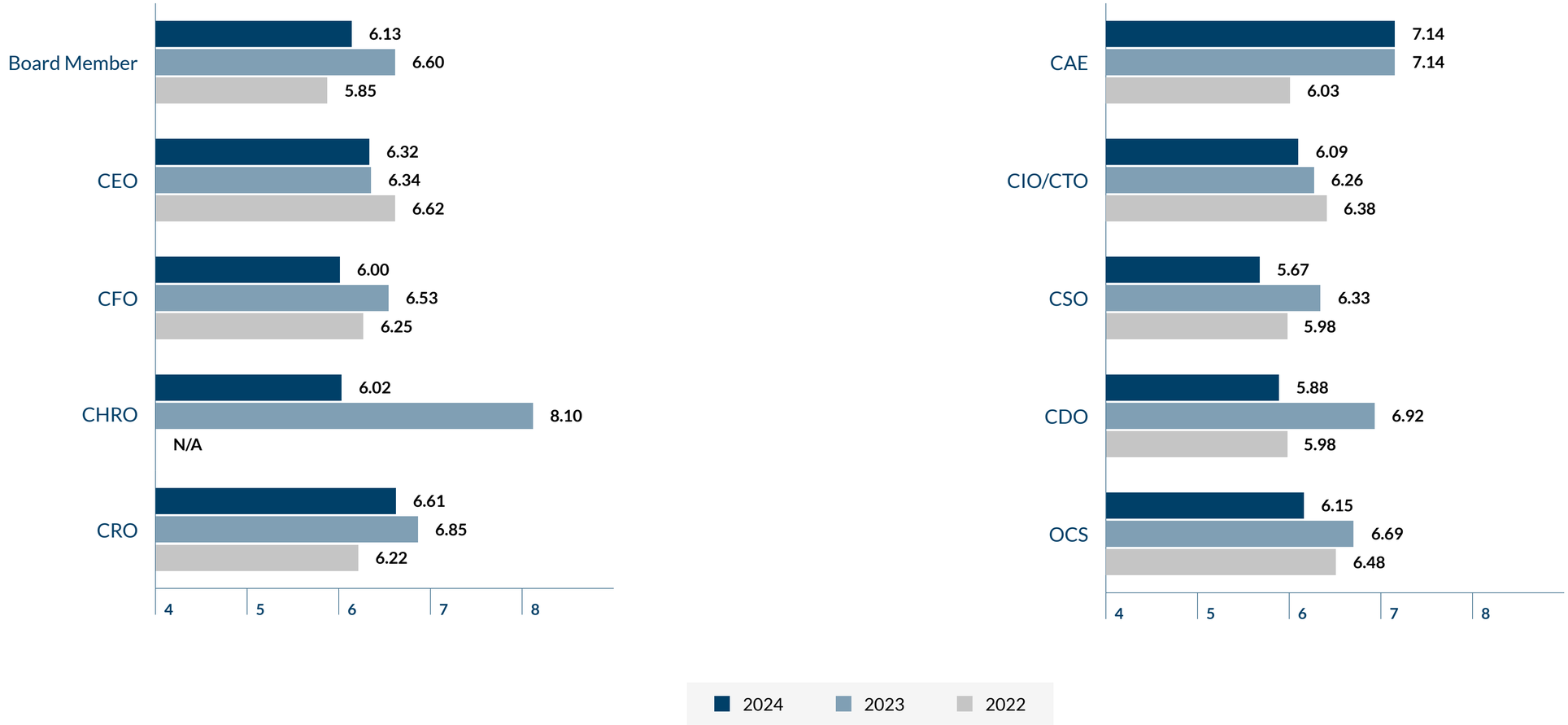
To determine if perspectives about top risks differ across executive positions, we separately examined responses received from board members and from nine executive positions. Similar to our analysis of the full sample and across the different sizes of organisations, we analyse responses about overall impressions of the magnitude and severity of risks across executive position held. The scores in Figure 9 reflect responses to the question about their overall impressions of the magnitude and severity of risks their organisation will be facing using a 10-point scale where 1 = "Extremely Low" and 10 = "Extremely High."

The overall impressions collectively across all executive positions with respect to the magnitude and severity of risks in the environment are that the level of risk looking forward to 2024 has decreased in comparison to last year's outlook for 2023. In addition, most groups view the risk environment for 2024 as lower than the outlook for 2022 two years ago. Only CEOs and CAEs have consistent future impressions of 2024 risk expectations relative to 2023, while all other positions see the 2024 risk outlook as lower than 2023. Except for the CSO and CDO positions, all other executive groups still have significant concerns about 2024, with each group rating the magnitude and severity of 2024 risks greater than 6.0 (i.e., the "Significant Impact" level), with CROs and CAEs rating the magnitude and severity of 2024 risks greater than 6.5.

The overall impressions collectively across all executive positions with respect to the magnitude and severity of risks in the environment are that the level of risk looking forward to 2024 has decreased in comparison to last year's outlook for 2023.

FIGURE 9

Overall, what is your impression of the magnitude and severity of risks your organisation will be facing with respect to achieving your performance goals over the next 12 months?



There is variation in perspectives across different executive positions, which suggests there may be significant value in explicitly discussing overall impressions about the risk environment among key leaders, especially at the highest level of the organisation. Enterprise risk assessments should benefit from the influx of multiple, diverse perspectives.

Consistent with prior reports, we use the colour-coding scheme below to highlight risks visually using three categories. In Table 10, we provide a summary of the impact assessments for each of the 36 risks for 2024 by category of executive using this colour-coding scheme:

Classification	Risks with an average score of	
Significant Impact	**6.0 or higher**	
Potential Impact	**4.51 through 5.99**	
Less Significant Impact	**4.5 or lower**	

"Boards clearly see talent and skills shortages as major concerns heading into 2024 and over the next decade. There also are indications that directors may perceive certain risks, such as succession and retention challenges as well as the skills required for adopting new technologies, as more significant than most C-suite leaders in their organisations. Clear and frequent communications between the board and executive team are critical to ensuring alignment of the organisation's strategic priorities."

EVELYN DILSAVER
INDEPENDENT DIRECTOR,
PROTIVITI ADVISORY BOARD MEMBER

TABLE 10

Role

Macroeconomic Risk Issues	Board	CEO	CFO	CHRO	CRO	CAE	CIO/ CTO	CSO	CDO	Other C-Suite
Economic conditions, including inflationary pressures	●	●	●	●	●	●	●	●	●	●
Impact of social issues and DEI priorities on ability to attract/ retain talent and compete	●	●	●	●	●	●	●	●	●	●
Increases in labour costs	●	●	●	●	●	●	●	●	●	●
Pandemic-related government policies and regulation	●	●	●	●	●	●	●	●	●	●
Volatility in global financial markets and currency exchange rates	●	●	●	●	●	●	●	●	●	●
Adoption of digital technologies requiring new skills in short supply	●	●	●	●	●	●	●	●	●	●
Geopolitical shifts, regional conflicts and instability in governmental regimes or expansion of global terrorism	●	●	●	●	●	●	●	●	●	●
Change in current interest rate environment	●	●	●	●	●	●	●	●	●	●
Changes in global markets and trade policies	●	●	●	●	●	●	●	●	●	●
Access to capital/liquidity	●	●	●	●	●	●	●	●	●	●

Strategic Risk Issues	Board	CEO	CFO	CHRO	CRO	CAE	CIO/ CTO	CSO	CDO	Other C-Suite
Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces	●	●	●	●	●	●	●	●	●	●
Heightened regulatory changes and scrutiny	●	●	●	●	●	●	●	●	●	●
Social media developments and platform technology innovations	●	●	●	●	●	●	●	●	●	●
Ease of entrance of new competitors or other changes in competitive environment	●	●	●	●	●	●	●	●	●	●
Organisation not sufficiently resilient and/or agile to manage an unexpected crisis	●	●	●	●	●	●	●	●	●	●
Limited opportunities for organic growth	●	●	●	●	●	●	●	●	●	●
Sustaining customer loyalty and retention	●	●	●	●	●	●	●	●	●	●
Growing focus on climate change and other sustainability policies, regulations, and expanding disclosure requirements as well as expectations of key stakeholders	●	●	●	●	●	●	●	●	●	●
Difficulty in growing through acquisitions, joint ventures and other activities	●	●	●	●	●	●	●	●	●	●
Substitute products and services that affect the viability of our business	●	●	●	●	●	●	●	●	●	●
Formulating business response to legal, political and social issues that are polarising	●	●	●	●	●	●	●	●	●	●
Performance shortfalls that trigger activist shareholders	●	●	●	●	●	●	●	●	●	●

Operational Risk Issues	Board	CEO	CFO	CHRO	CRO	CAE	CIO/ CTO	CSO	CDO	Other C-Suite
Third-party risks	●	●	●	●	●	●	●	●	●	●
Ability to attract, develop and retain top talent, manage shifts in labour expectations, and address succession challenges	●	●	●	●	●	●	●	●	●	●
Cyber threats	●	●	●	●	●	●	●	●	●	●
Ensuring privacy and compliance with growing identity protection expectations	●	●	●	●	●	●	●	●	●	●
Existing operations and legacy IT infrastructure unable to meet performance expectations as well as “born digital” competitors	●	●	●	●	●	●	●	●	●	●
Uncertainty surrounding core supply chain ecosystem	●	●	●	●	●	●	●	●	●	●
Inability to utilise rigorous data analytics to achieve market intelligence and increase productivity and efficiency	●	●	●	●	●	●	●	●	●	●
Meeting expectations around protecting health and safety of employees (including their well-being and mental health), customers, suppliers and our communities	●	●	●	●	●	●	●	●	●	●
Enhanced exposure to fraud in the industry	●	●	●	●	●	●	●	●	●	●
Challenges in sustaining culture due to changes in overall work environment	●	●	●	●	●	●	●	●	●	●
Resistance to change restricting organisation from adjusting business model and core operations	●	●	●	●	●	●	●	●	●	●

Operational Risk Issues (continued)	Board	CEO	CFO	CHRO	CRO	CAE	CIO/ CTO	CSO	CDO	Other C-Suite
Managing demands on or expectations of workforce to work remotely or as part of a hybrid work environment	●	●	●	●	●	●	●	●	●	●
Organisation's culture not sufficiently encouraging timely identification and escalation of emerging risk issues	●	●	●	●	●	●	●	●	●	●
Rising threat of catastrophic natural disasters and weather phenomena	●	●	●	●	●	●	●	●	●	●

2024 risk issues

In relation to our prior year results, almost every group of executives reduced the number of risks they rated as "Significant Impact." Board members decreased their "Significant Impact" risks from four in 2023 to zero in 2024. Other groups also report declines in "Significant Impact" risks after the heightened concern over the two previous years. CEOs report zero risks at the highest impact level, down from five in 2023 and 11 in 2022. Somewhat surprisingly, CFOs report nine of the 36 risks as "Less Significant Impact," more than any other executive group. These results help explain the slight decrease in the overall magnitude and severity results for 2024 relative to the prior year.

While there is some consistency, there are also noticeable differences in views about 2024 risk conditions across executive type. Most positions (eight of 10) identify concerns related to attracting and developing talent and to the economy as top five risks. Interestingly, CHROs did not include concerns related to attracting talent as a top five risk concern. CSOs and CDOs are the only two positions to not identify the economy as a top five risk issue.

There is general agreement in the relative significance among specific risks between CEOs and board members, given that all of the 36 risks are rated at the "Potential Impact" level (4.51 through 5.99) by both groups, except for one risk that CEOs rate at the "Less Significant Impact" level (4.50 or lower). There is general agreement among boards and CEOs in the top five risks, given that four of the top five risks are the same for both positions.

CFOs have somewhat differing views about the top risks compared to boards and CEOs, given that CFOs, unlike these other two groups, highlight concerns related to labour costs and the changing current interest rate environment as top five risk issues. CFOs are the most optimistic about 2024 — they rate nine of the 36 risks at the "Less Significant Impact" level. Unlike board members and CFOs, CEOs identify risks related to heightened regulatory changes and scrutiny among their top five risk issues for 2024.

For 2024, only CHROs, CROs and CAEs view any of the risks at the "Significant Impact" level. Interestingly, however, there is variation across those three groups as to the nature of the risks at that level, suggesting they see differences in the relative significance of specific risks. The one exception is third-party risks, which CROs, CAEs and CHROs all rate at the "Significant Impact" level.

As noted earlier, varying perspectives among executives and directors call for more discussion among executive members in order to better understand how each group views the risk landscape and obtain a clearer view of the organisation's risk profile.

2034 risk issues

For a decade out (2034), overall risk perceptions exhibit significant variation relative to 2024. Board members rate three of their top five risk issues at the "Significant Impact" level, while CEOs, CFOs and CROs rate none of their top five risks at that level. CAEs have the most concern about the future, rating 15 risks at the "Significant Impact" level, including eight of the 14 operational risks. Further, CAEs rate all top five risks at 7.0 or higher. This is significantly more than any other executive group. On the other hand, only CFOs rate more than one risk as having a "Less Significant Impact" in 2034. Overall, the 2034 results show an increase in risk concerns for 2034 relative to the short-term risk concerns summarised above.

There is general agreement in the long-term top five risks for boards and CEOs, with technology-themed risks comprising three of their top five issues. Additionally, all positions — except CFOs — include cyber threats as a top five risk, with six of 10 positions rating that risk in the number one or two position for long-term risk issues. Eight of the 10 positions also include concerns about the adoption of digital technologies requiring skills in short supply as a top five risk issue a decade from now. Six of 10 positions include concerns about the rapid speed of disruptive innovation as a long-term top five risk issue. Technology- and innovation-related risks are a common theme for long-term horizons.

Table 11 shows a summary of the impact assessments for each of the 36 risks for both 2024 and 2034 to highlight differences in views about individual risks across different executive positions.

Varying perspectives among executives and directors call for more discussion among executive members in order to better understand how each group views the risk landscape and obtain a clearer view of the organisation's risk profile.

TABLE 11

Perceived impact for 2024 and 2034 — by role

Macroeconomic Risk Issues	Year	Board	CEO	CFO	CHRO	CRO	CAE	CIO/ CTO	CSO	CDO	Other C-Suite
Economic conditions, including inflationary pressures	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Impact of social issues and DEI priorities on ability to attract/ retain talent and compete	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Increases in labour costs	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Pandemic-related government policies and regulation	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Volatility in global financial markets and currency exchange rates	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Adoption of digital technologies requiring new skills in short supply	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Geopolitical shifts, regional conflicts and instability in governmental regimes or expansion of global terrorism	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●

Macroeconomic Risk Issues (continued)	Year	Board	CEO	CFO	CHRO	CRO	CAE	CIO/ CTO	CSO	CDO	Other C-Suite
Change in current interest rate environment	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Changes in global markets and trade policies	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Access to capital/liquidity	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●

Strategic Risk Issues	Year	Board	CEO	CFO	CHRO	CRO	CAE	CIO/ CTO	CSO	CDO	Other C-Suite
Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Heightened regulatory changes and scrutiny	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Social media developments and platform technology innovations	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Ease of entrance of new competitors or other changes in competitive environment	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●

Strategic Risk Issues (continued)	Year	Board	CEO	CFO	CHRO	CRO	CAE	CIO/ CTO	CSO	CDO	Other C-Suite
Organisation not sufficiently resilient and/or agile to manage an unexpected crisis	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Limited opportunities for organic growth	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Sustaining customer loyalty and retention	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Growing focus on climate change and other sustainability policies, regulations, and expanding disclosure requirements as well as expectations of key stakeholders	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Difficulty in growing through acquisitions, joint ventures and other activities	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Substitute products and services that affect the viability of our business	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Formulating business response to legal, political and social issues that are polarising	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Performance shortfalls that trigger activist shareholders	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●

Operational Risk Issues	Year	Board	CEO	CFO	CHRO	CRO	CAE	CIO/ CTO	CSO	CDO	Other C-Suite
Third-party risks	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Ability to attract, develop and retain top talent, manage shifts in labour expectations, and address succession challenges	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Cyber threats	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Ensuring privacy and compliance with growing identity protection expectations	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Existing operations and legacy IT infrastructure unable to meet performance expectations as well as “born digital” competitors	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Uncertainty surrounding core supply chain ecosystem	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Inability to utilise rigorous data analytics to achieve market intelligence and increase productivity and efficiency	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Meeting expectations around protecting health and safety of employees (including their well-being and mental health), customers, suppliers and our communities	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●

Operational Risk Issues (continued)	Year	Board	CEO	CFO	CHRO	CRO	CAE	CIO/ CTO	CSO	CDO	Other C-Suite
Enhanced exposure to fraud in the industry	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Challenges in sustaining culture due to changes in overall work environment	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Resistance to change restricting organisation from adjusting business model and core operations	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Managing demands on or expectations of workforce to work remotely or as part of a hybrid work environment	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Organisation's culture not sufficiently encouraging timely identification and escalation of emerging risk issues	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●
Rising threat of catastrophic natural disasters and weather phenomena	2024	●	●	●	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●	●	●	●

Figures 10-19 on the following pages highlight the top five risks identified by board members and each executive position (collectively referred to as "leadership positions"). For 2024, eight of the 10 leadership positions (except for CHROs and CDOs) rank concerns about succession challenges and the ability to attract and retain top talent along with uncertainty regarding current economic conditions in their top five risks for 2024. Succession challenges and retaining top talent is rated the top risk by board members and CFOs, while CEOs, CHROs and OCS position groups list concerns about economic conditions as their top risk. Unease about the organisation's ability to manage cyber threats, such as ransomware and other attacks, is also recognised by six of the position groups.

For 2024, CHROs, CROs and CAEs rate each of their top five risks at the "Significant Impact" level; however, no other leadership position group rates any of the top five risks at this level. While most position groups share a number of top five risks, one position group has a unique set of risks. CDOs are focused on a distinctive set of risks for 2024, citing social media developments, data analytics, social issues and DEI, geopolitical shifts, and the rising threat of catastrophic natural disasters. CSOs also list three other unique risks (all strategic) in their top five rankings. Overall, the results reflect how different roles offer varying perspectives when assessing risks in disparate environments and over longer versus shorter time horizons.

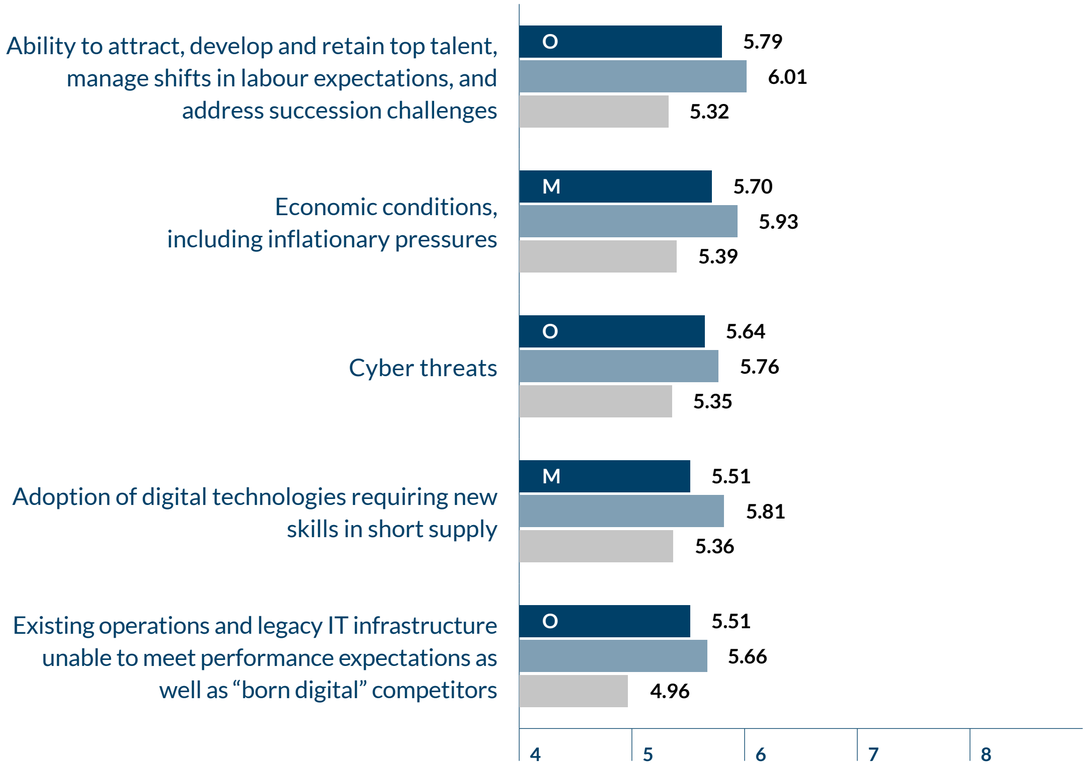
Nineteen of the 36 risks that appear as top five risk concerns for 2024 are cited by at least one of the position groups. Within this collective group of top five risk concerns, there are six of the 10 macroeconomic risks, eight of the 14 operational risks and five of the 12 strategic risks. Of the three risks cited by at least half of the position groups, two are operational risks and the other is a macroeconomic risk.

Looking out to 2034, four risks are common top five risks across the majority of position groups: (1) worries that the organisation may not be sufficiently prepared to meet cyber threats, (2) concerns about succession challenges and the ability to attract and retain top talent, (3) concerns that the adoption of digital strategies will require new skills that are in short supply, and (4) concerns about the rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces. For 2034, 15 of the 36 risks that appear as top five risks are cited by at least one of the position groups, with four being macroeconomic, five strategic and six operational.

These results prominently reflect the importance of bringing varying perspectives to the enterprise risk management (ERM) process. Each executive is needed to best identify and assess risks in disparate environments and over longer versus shorter time horizons. It is of paramount importance that both the board and management team engage in dialogue regarding the most critical enterprise risks, given the different perspectives each brings to the table and the potential for a lack of consensus. Without clarity of focus, the executive team may not be aligned both internally and with the board on what the top risks are. Worse, they may not be appropriately addressing the most important risks facing the organisation, thereby leaving the organisation potentially vulnerable to certain risk events.

FIGURE 10A

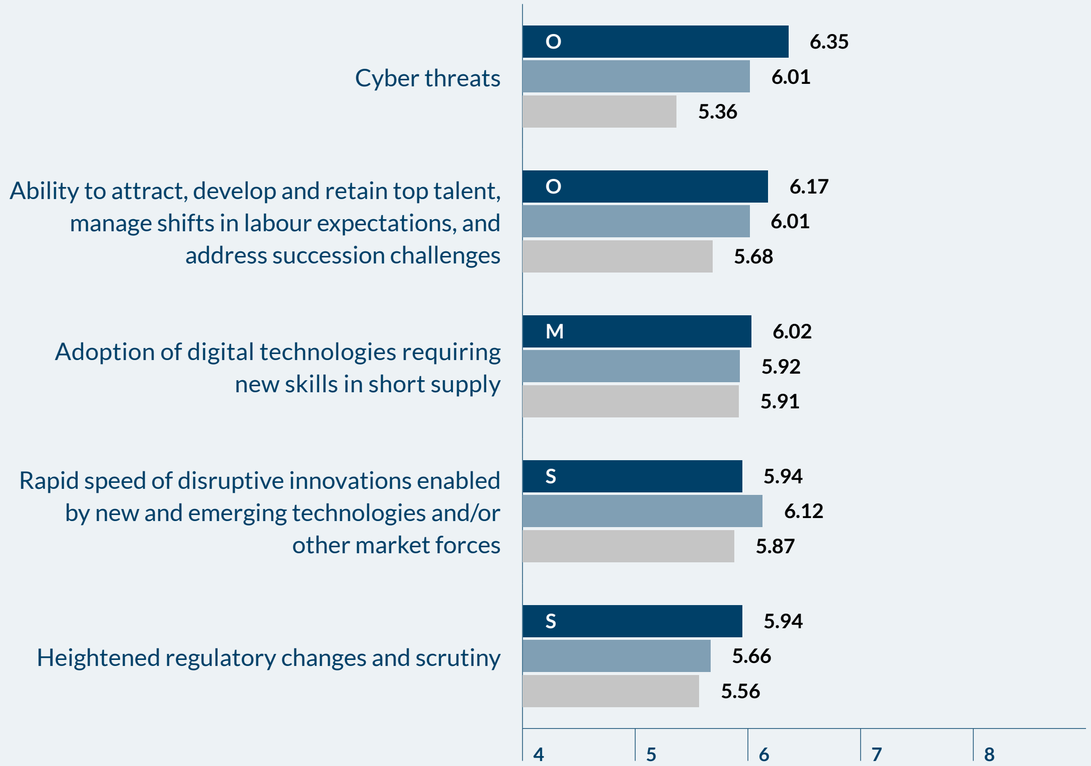
Board Members — 2024



M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue 2024 2023 2022

FIGURE 10B

Board Members — 2034



M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue 2034 2033* 2032*

* 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.

FIGURE 11A

CEOs — 2024

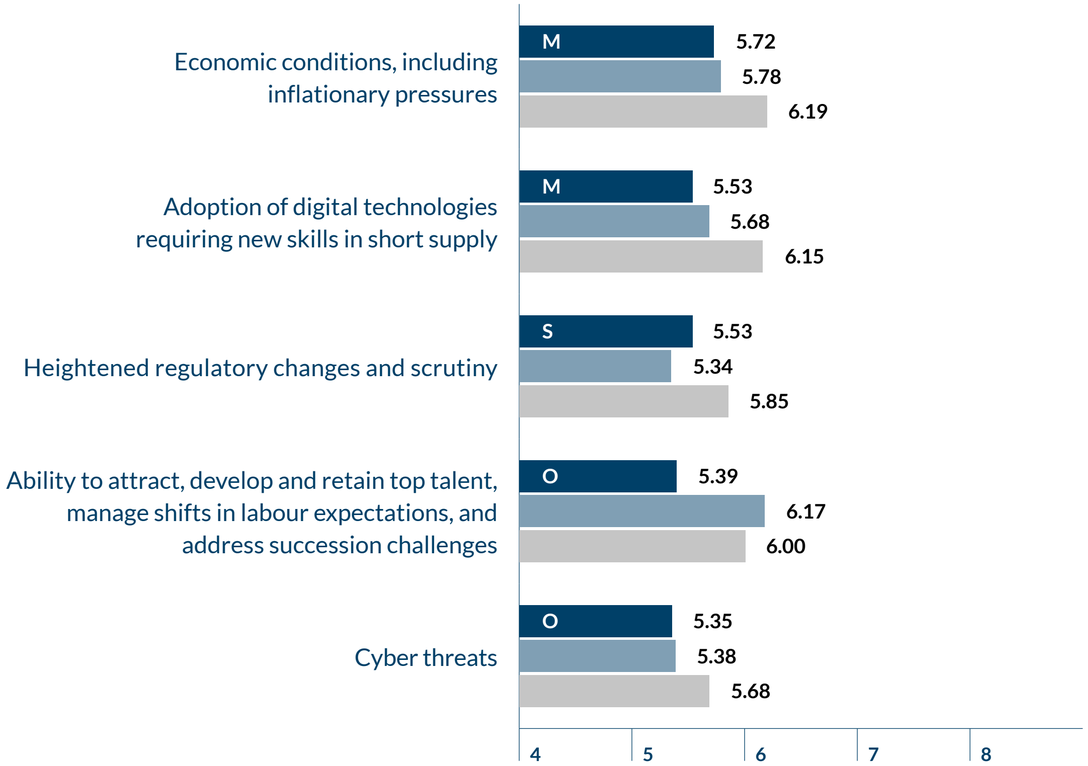
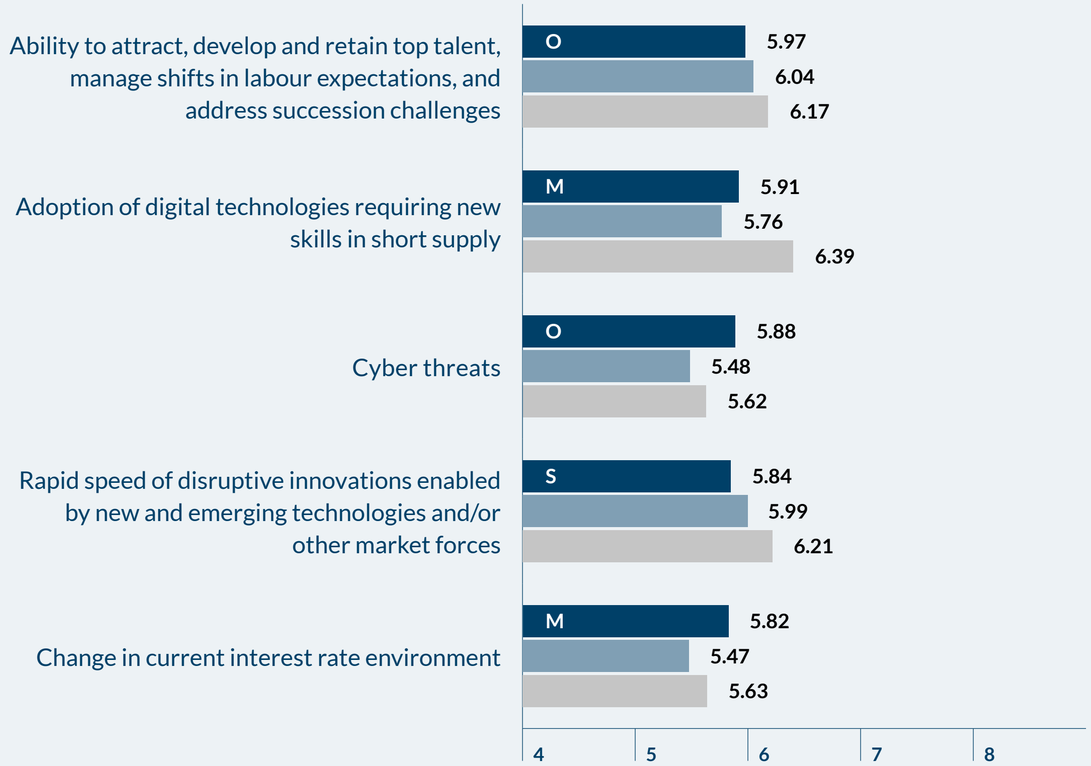


FIGURE 11B

CEOs — 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.

FIGURE 12A

CFOs — 2024

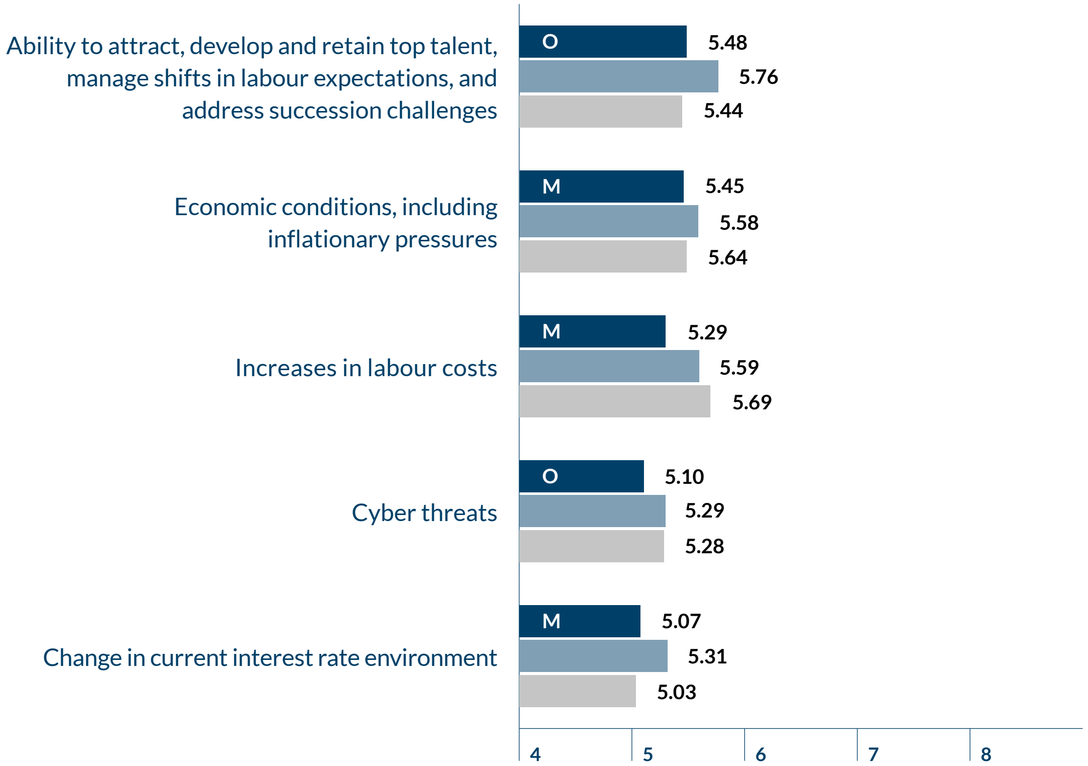
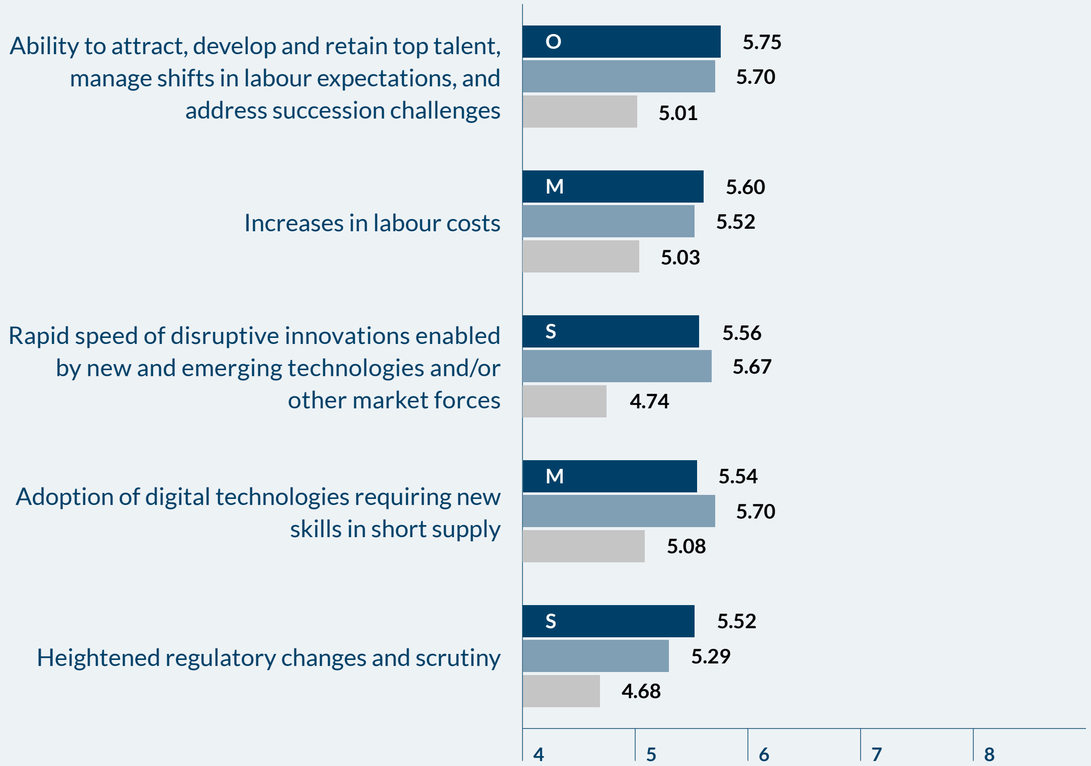


FIGURE 12B

CFOs — 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.

FIGURE 13A

CROs — 2024

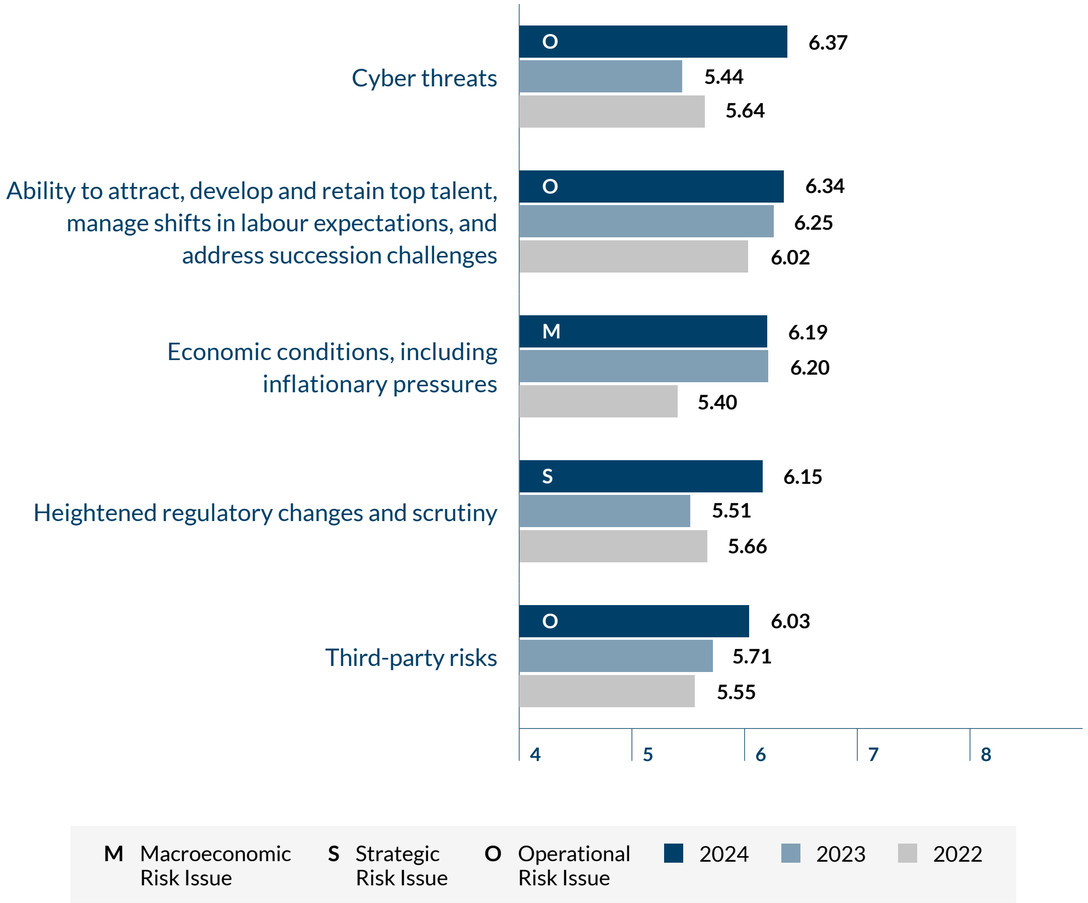
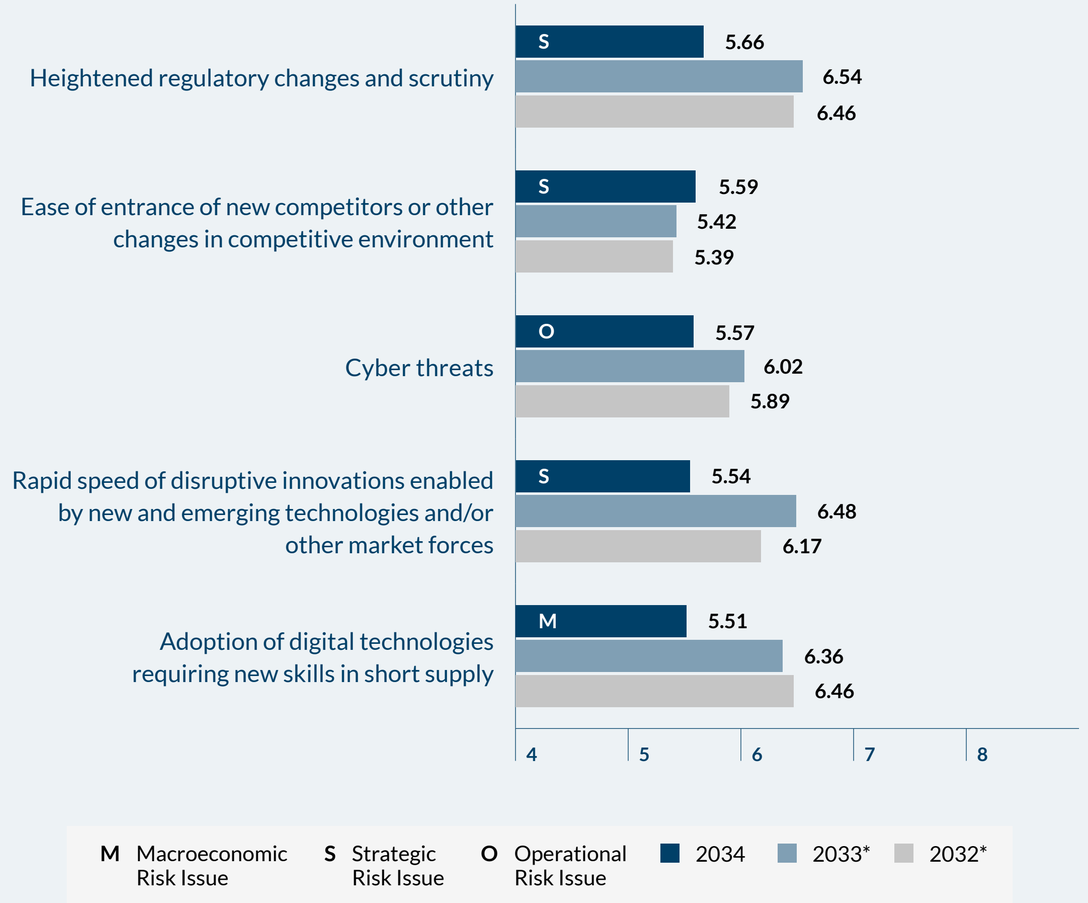


FIGURE 13B

CROs — 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.

FIGURE 14A

CAEs — 2024

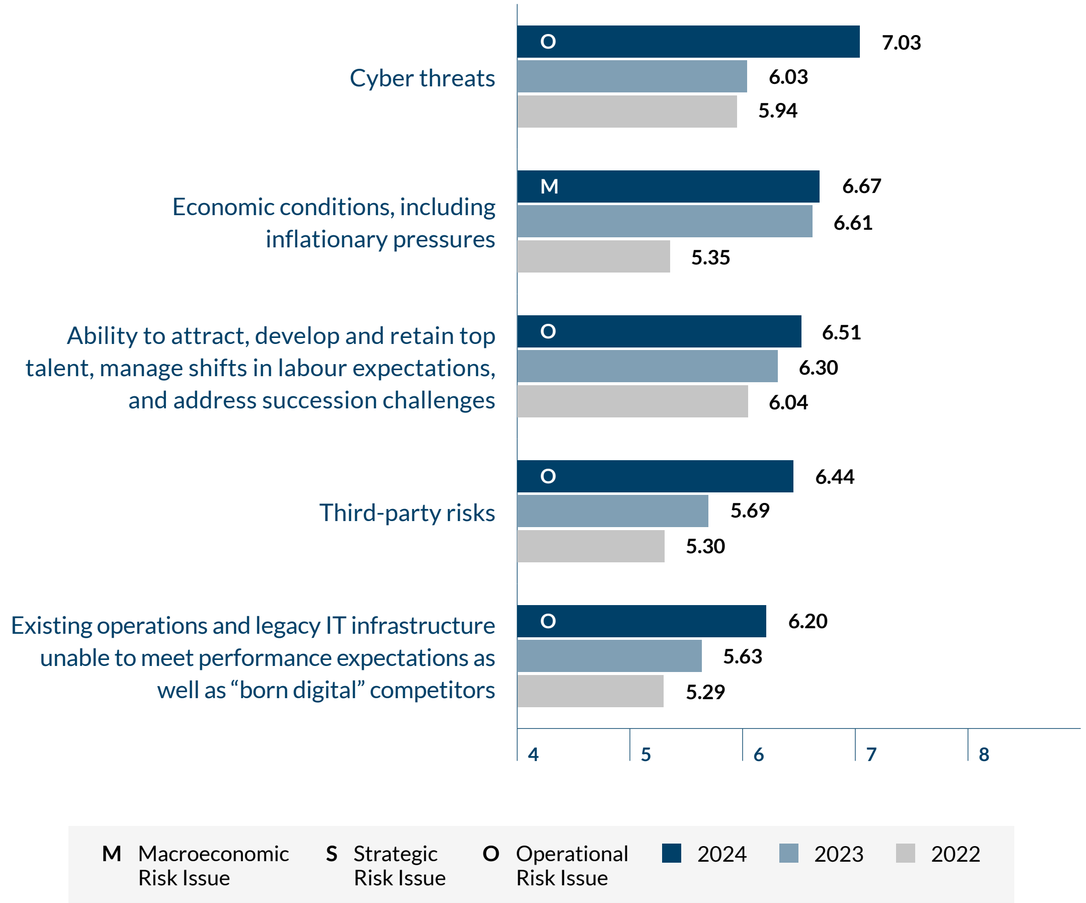
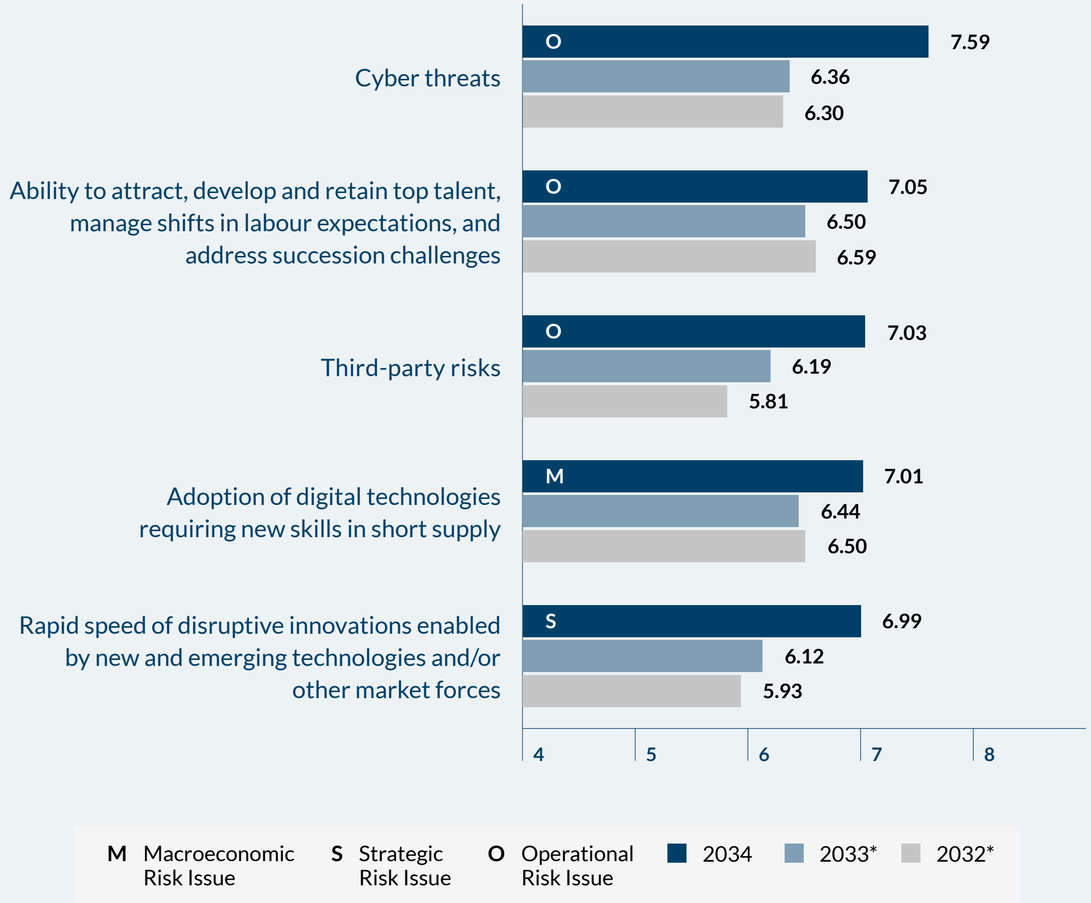


FIGURE 14B

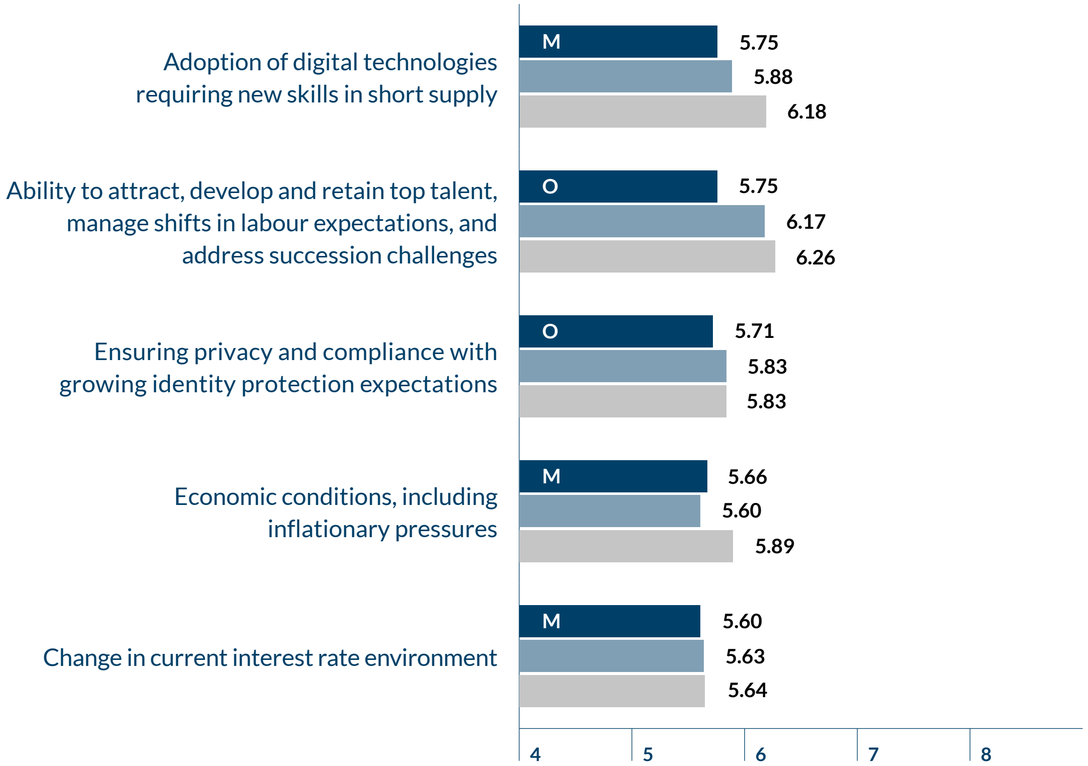
CAEs — 2034



* 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.

FIGURE 15A

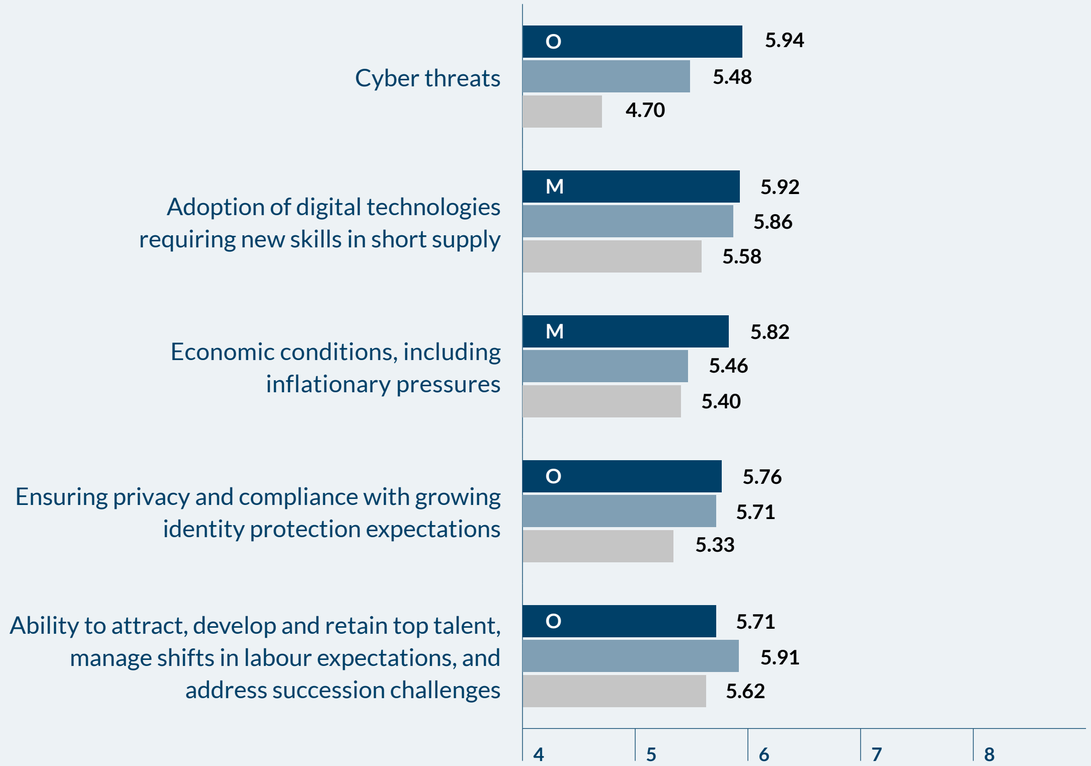
CIOs/CTOs — 2024



M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue 2024 2023 2022

FIGURE 15B

CIOs/CTOs — 2034

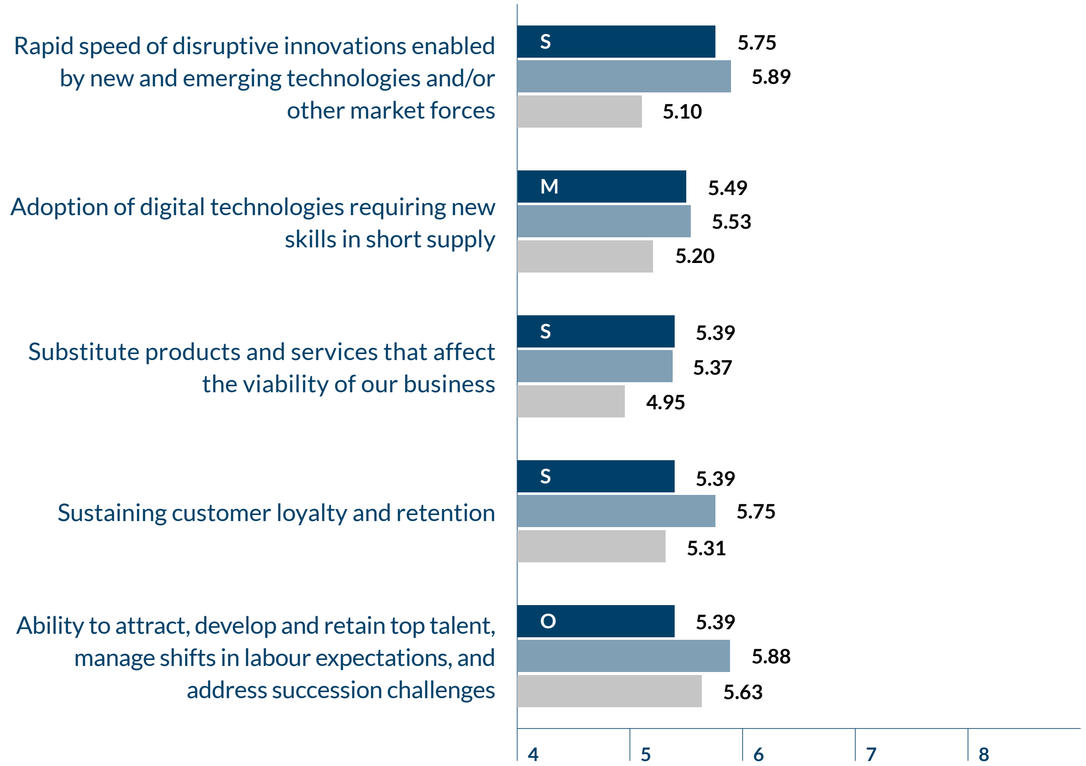


M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue 2034 2033* 2032*

* 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.

FIGURE 16A

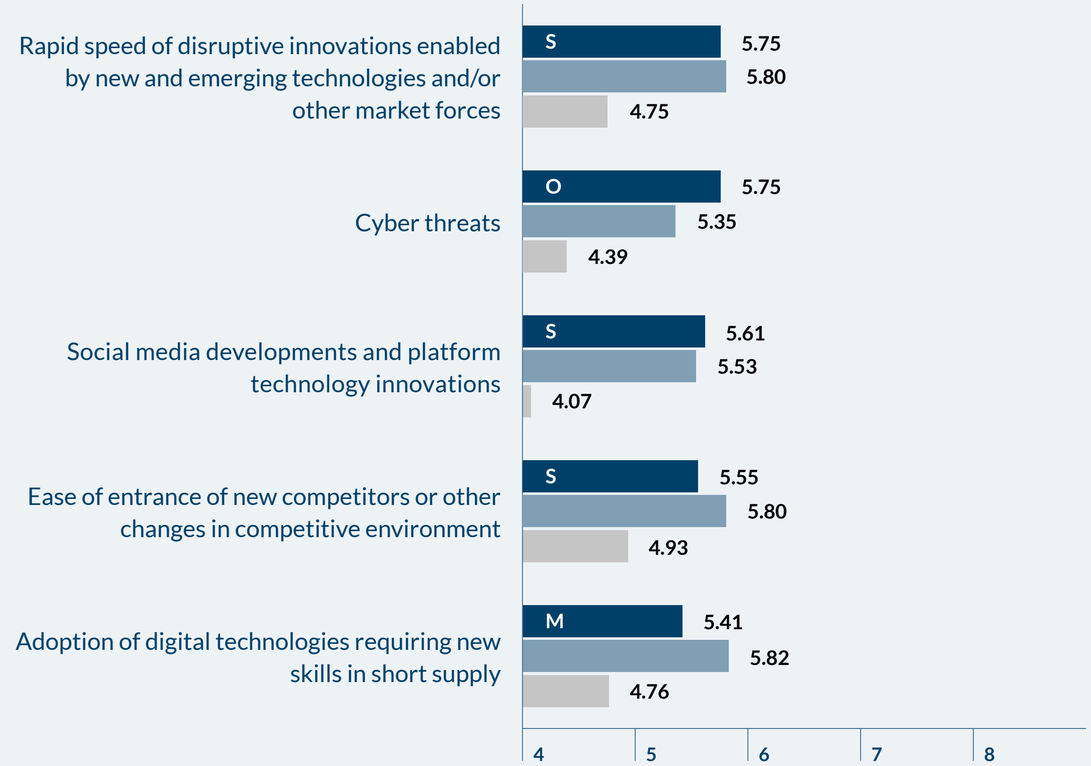
CSOs — 2024



M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue 2024 2023 2022

FIGURE 16B

CSOs — 2034



M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue 2034 2033* 2032*

* 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.

FIGURE 17A

CDOs — 2024

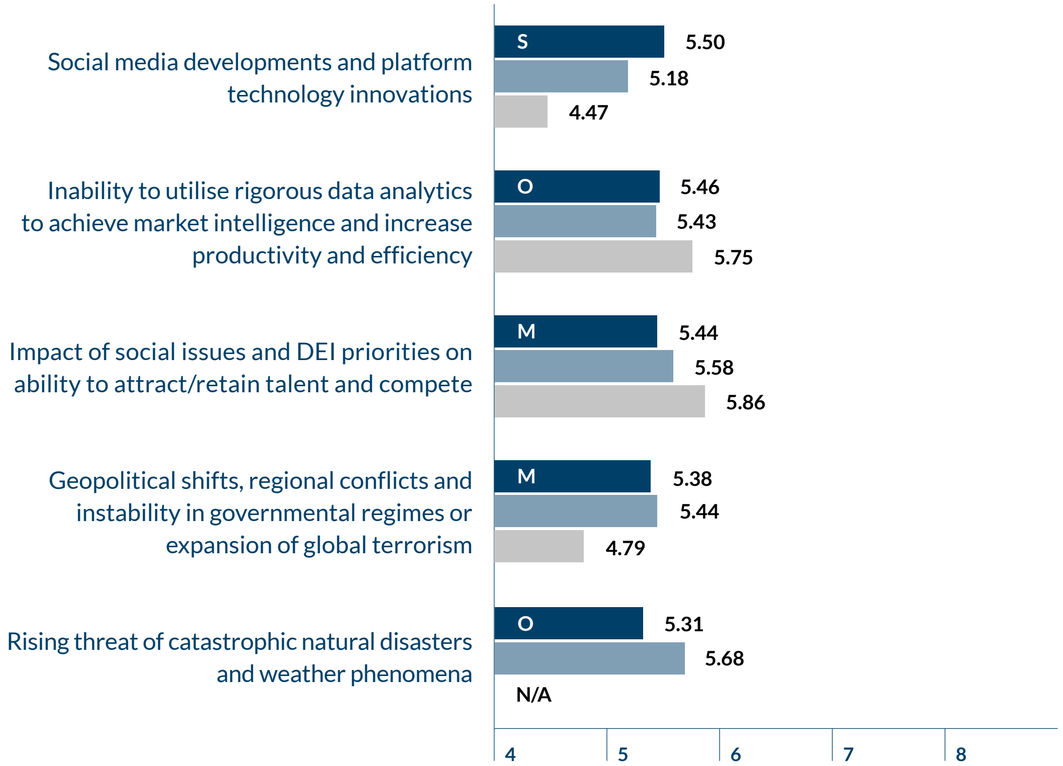
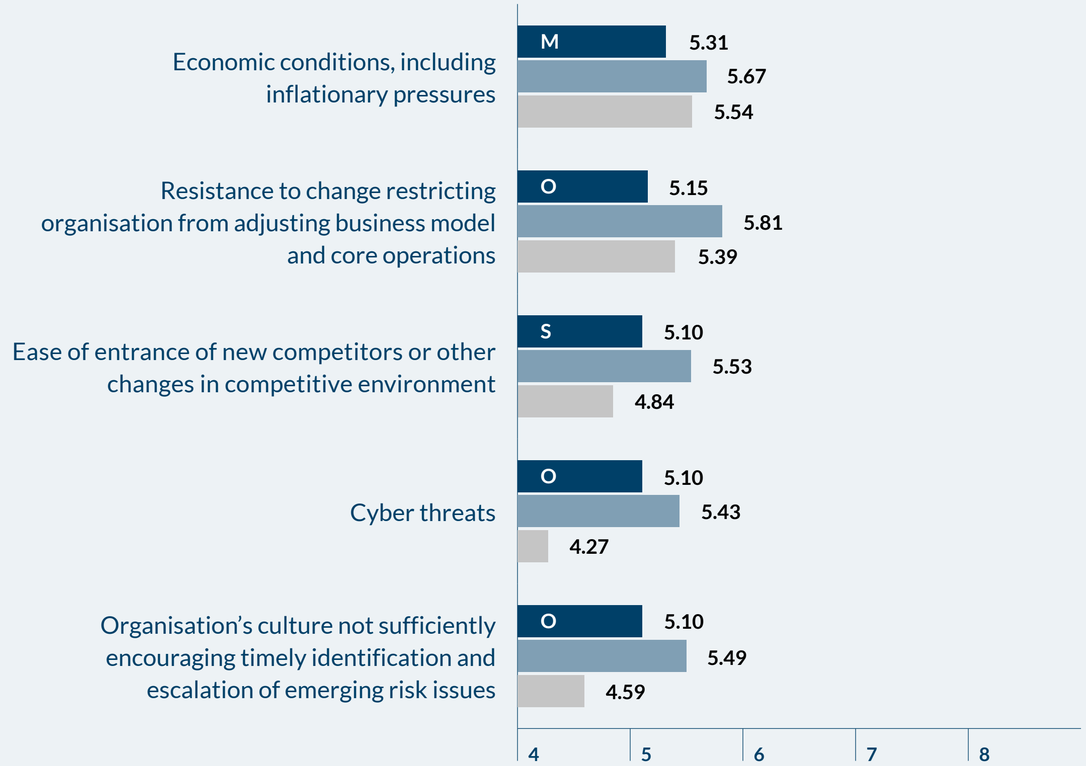


FIGURE 17B

CDOs — 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.

FIGURE 18A

CHROs — 2024

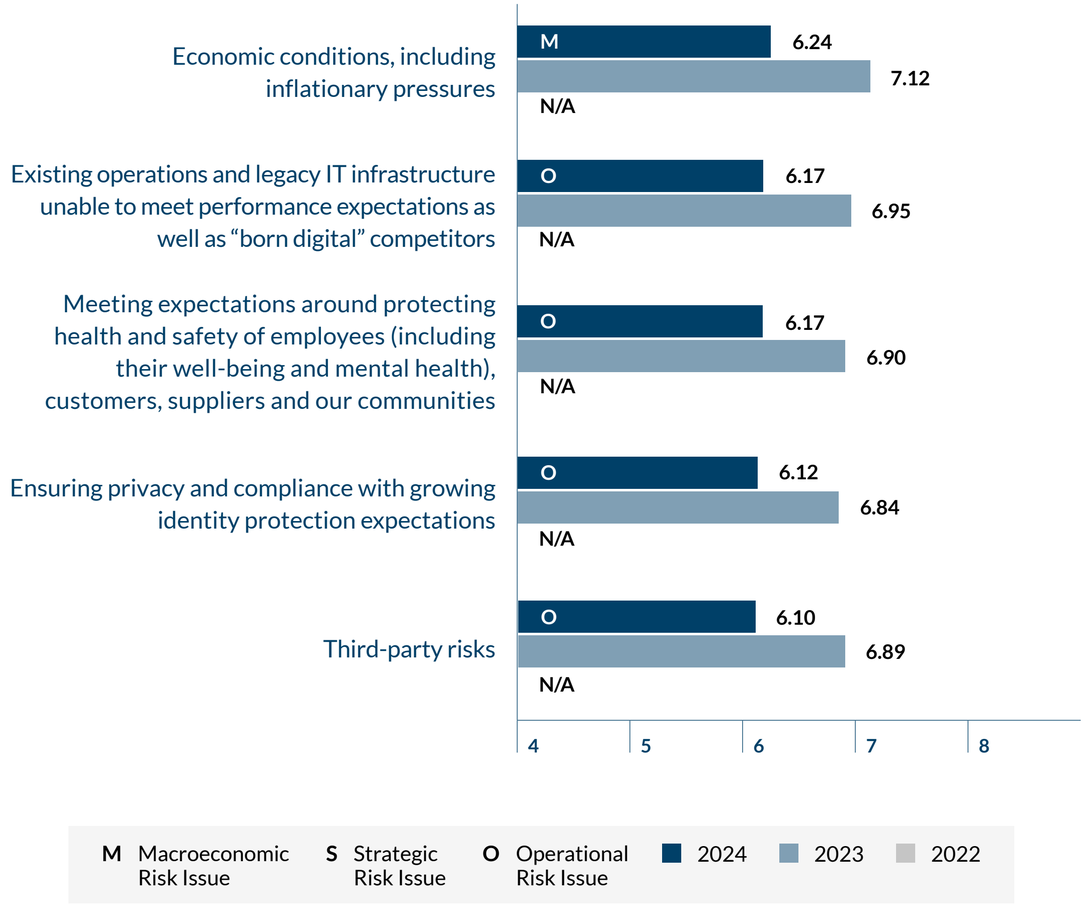
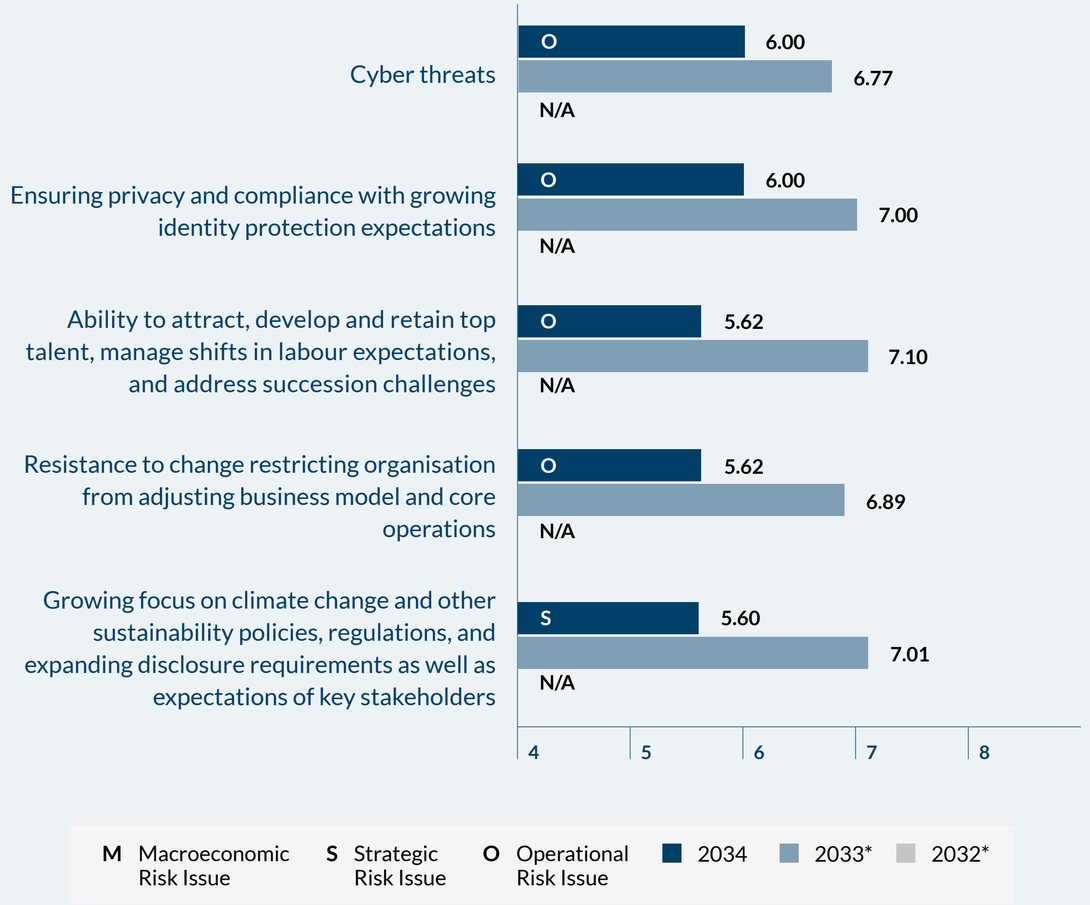


FIGURE 18B

CHROs — 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.

FIGURE 19A

Other C-Suite — 2024

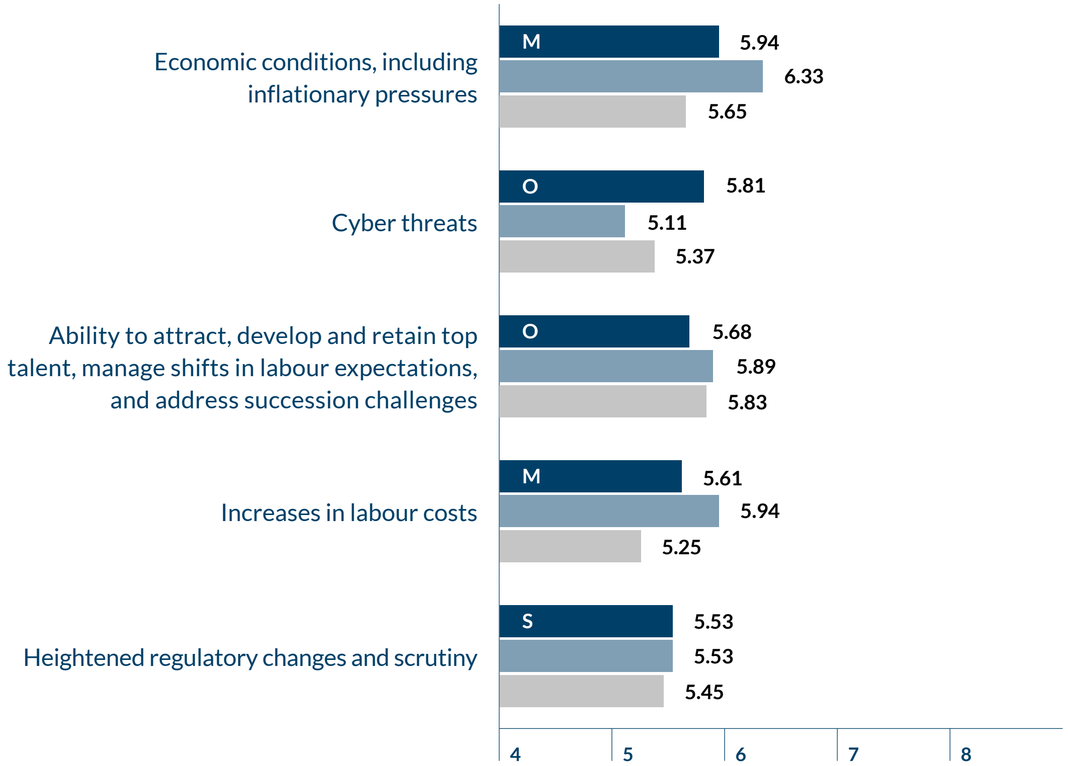
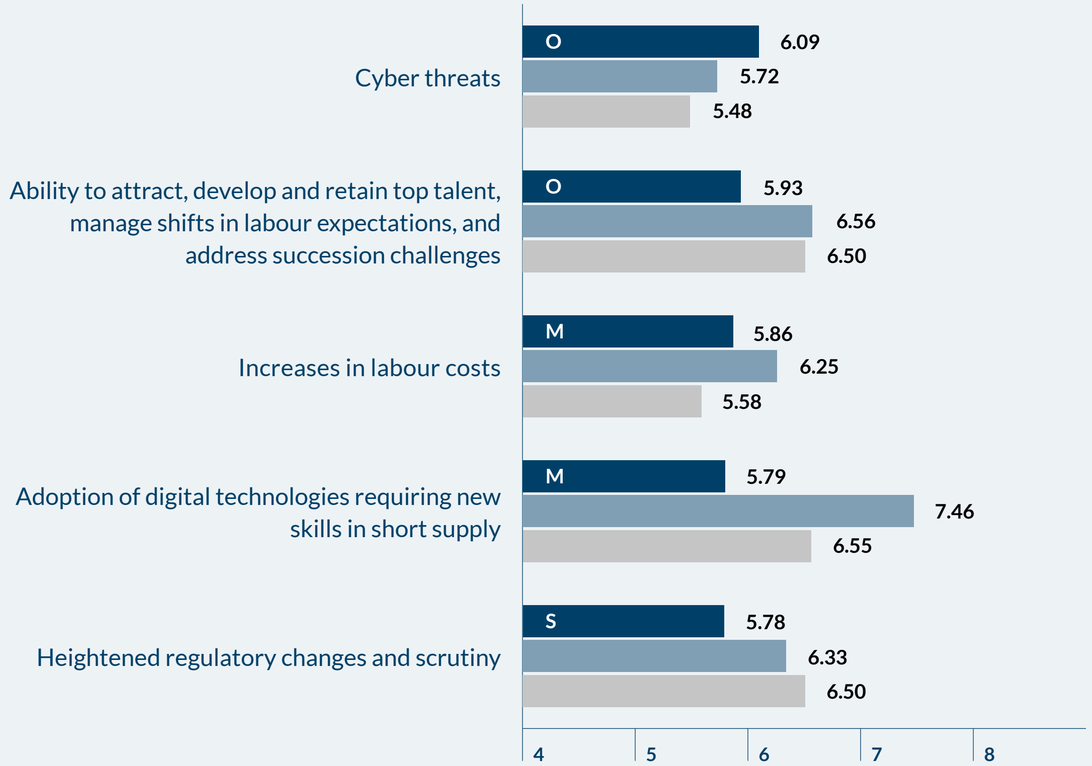


FIGURE 19B

Other C-Suite — 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.

Analysis across industry groups

What you need to know

What they see: Most industry groups perceive the magnitude and severity of risks their organisations face will be lower as they look ahead to 2024 relative to 2023.

- However, all industry groups still see the overall riskiness of the business environment as higher (or as high) as 2022.

Differing perceptions by industry: Among the notable industry risk concerns for 2024:

- The Healthcare industry group rates the most risks at the "Significant Impact" level — these include cyber threats, data privacy, third-party risks and talent shortages.
- Financial services respondents rate four of the 36 risks at the "Significant Impact" level — overall economic conditions, the current interest rate environment, heightened regulatory scrutiny and cyber threats.
- Energy and Utilities organisations believe that 2024 will be riskier than 2023.
- Three of the seven industry groups rate cyber threats as a "Significant Impact" risk.

The next decade is riskier: The significance of risk concerns a decade out is higher than short-term risk concerns.

- For five of the seven industry groups, all of the top five risks for 2034 are at the "Significant Impact" level.
- Cyber threats and attracting, developing and retaining top talent, including succession challenges, are in the top five risks for all industry groups.
- Rising threat of catastrophic natural disasters and weather phenomena is a top five long-term risk concern for Energy and Utilities and Government Agencies.

Important takeaway: These noted differences in perceptions of risk issues across the different industry groups highlight the importance of understanding industry drivers and emerging developments to identify the most significant enterprise risks and emerging risk concerns in each group.

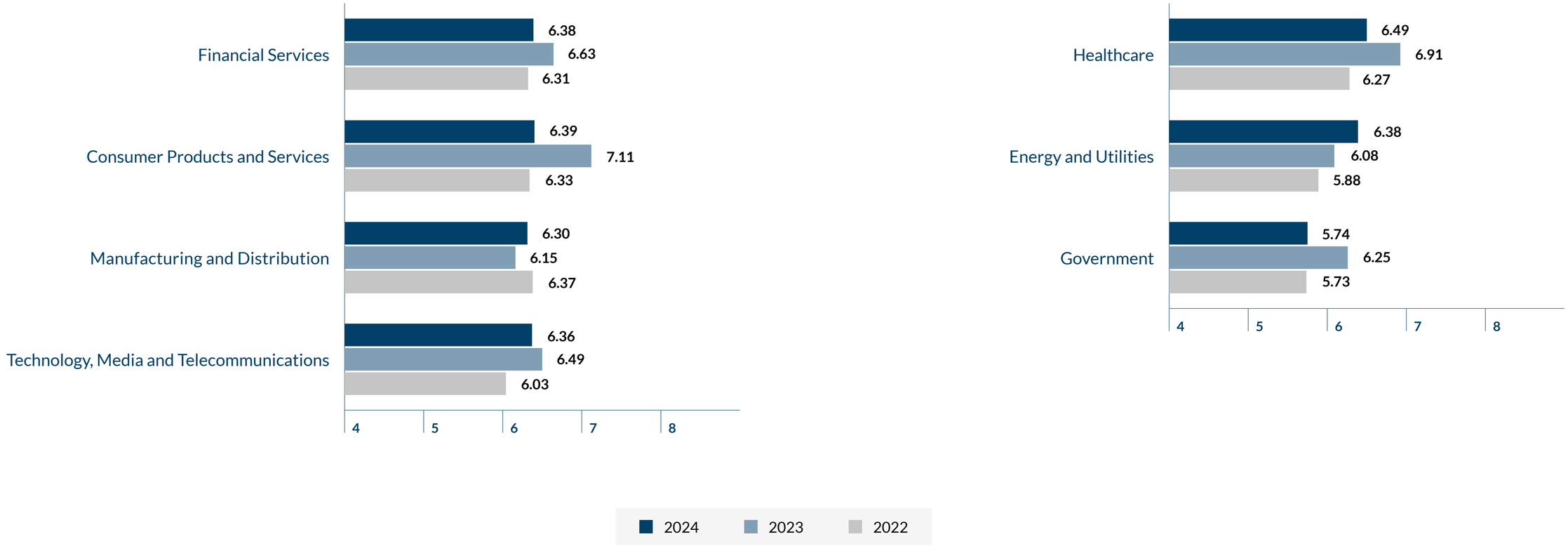
We analyse responses across seven industry groups to determine whether industries rank-order risks differently. Similar to our analysis of the full sample and across different types of respondents, we analyse responses about overall impressions of the magnitude and severity of risks across industry groups.

Industry group	Number of respondents
Financial Services (FS)	241
Consumer Products and Services (CPS)	218
Manufacturing and Distribution (MD)	217
Technology, Media and Telecommunications (TMT)	120
Healthcare (HC)	104
Energy and Utilities (EU)	112
Governmental Agencies (GOVT)	43
Other industries (not separately reported)	88
Total number of respondents	**1,143**

The scores below in Figure 20 reflect responses using a 10-point scale where 1 = “Extremely Low” and 10 = “Extremely High.”

FIGURE 20

Overall, what is your impression of the magnitude and severity of risks your organisation will be facing with respect to achieving your performance goals over the next 12 months?



With the exception of the Energy and Utilities and Manufacturing and Distribution industry groups, respondents in all other industry groups perceive the magnitude and severity of risks their organisations face will be lower as they look ahead to 2024 relative to 2023; however, most industry groups still see the overall riskiness of the business environment as higher (or as high) as 2022. In addition, industry groups are consistent in their belief that risks in 2024 will have a "Significant Impact," with the only exception being Government, which had an overall magnitude and severity score below 6.0. This suggests there is an overall concern for the short-term future, something that should be noted when considering additional data.

Consistent with prior reports, we use the colour-coding scheme in the accompanying table to highlight risks visually using three categories. In Table 12, we provide a summary of the impact assessments for each of the 36 risks for 2024 by industry group using this colour-coding scheme:

Classification	Risks with an average score of	
Significant Impact	**6.0 or higher**	●
Potential Impact	**4.51 through 5.99**	●
Less Significant Impact	**4.5 or lower**	●

Table 12 shows the average risk scores for 2024 to highlight differences in views about individual risks across different industry groups. In Table 13, we show 2034 results.

TABLE 12

Industry

Macroeconomic Risk Issues	FS	CPS	MD	TMT	HC	EU	GOVT
Economic conditions, including inflationary pressures	●	●	●	●	●	●	●
Increases in labour costs	●	●	●	●	●	●	●
Change in current interest rate environment	●	●	●	●	●	●	●
Adoption of digital technologies requiring new skills in short supply	●	●	●	●	●	●	●
Access to capital/liquidity	●	●	●	●	●	●	●
Impact of social issues and DEI priorities on ability to attract/retain talent and compete	●	●	●	●	●	●	●
Geopolitical shifts, regional conflicts and instability in governmental regimes or expansion of global terrorism	●	●	●	●	●	●	●
Volatility in global financial markets and currency exchange rates	●	●	●	●	●	●	●
Changes in global markets and trade policies	●	●	●	●	●	●	●
Pandemic-related government policies and regulation	●	●	●	●	●	●	●

Strategic Risk Issues	FS	CPS	MD	TMT	HC	EU	GOVT
Heightened regulatory changes and scrutiny	🔴	🟡	🟡	🟡	🔴	🟡	🟡
Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces	🟡	🟡	🟡	🟡	🟡	🟡	🟡
Organisation not sufficiently resilient and/or agile to manage an unexpected crisis	🟡	🟡	🟡	🟡	🟡	🟡	🟡
Limited opportunities for organic growth	🟡	🟡	🟡	🟡	🟡	🟡	🟡
Sustaining customer loyalty and retention	🟡	🟡	🟡	🟡	🟡	🟢	🟡
Formulating business response to legal, political and social issues that are polarising	🟡	🟡	🟡	🟡	🟡	🟢	🟡
Social media developments and platform technology innovations	🟡	🟡	🟡	🟡	🟡	🟢	🟡
Growing focus on climate change and other sustainability policies, regulations, and expanding disclosure requirements as well as expectations of key stakeholders	🟡	🟡	🟡	🟡	🟢	🟡	🟡
Ease of entrance of new competitors or other changes in competitive environment	🟡	🟡	🟡	🟡	🟡	🟢	🟡
Difficulty in growing through acquisitions, joint ventures and other activities	🟡	🟡	🟡	🟡	🟡	🟡	🟢
Substitute products and services that affect the viability of our business	🟡	🟡	🟡	🟡	🟡	🟢	🟢
Performance shortfalls that trigger activist shareholders	🟡	🟡	🟡	🟡	🟡	🟢	🟡

Operational Risk Issues	FS	CPS	MD	TMT	HC	EU	GOVT
Cyber threats	●	●	●	●	●	●	●
Ability to attract, develop and retain top talent, manage shifts in labour expectations, and address succession challenges	●	●	●	●	●	●	●
Third-party risks	●	●	●	●	●	●	●
Ensuring privacy and compliance with growing identity protection expectations	●	●	●	●	●	●	●
Challenges in sustaining culture due to changes in overall work environment	●	●	●	●	●	●	●
Existing operations and legacy IT infrastructure unable to meet performance expectations as well as "born digital" competitors	●	●	●	●	●	●	●
Inability to utilise rigorous data analytics to achieve market intelligence and increase productivity and efficiency	●	●	●	●	●	●	●
Resistance to change restricting organisation from adjusting business model and core operations	●	●	●	●	●	●	●
Organisation's culture not sufficiently encouraging timely identification and escalation of emerging risk issues	●	●	●	●	●	●	●
Meeting expectations around protecting health and safety of employees (including their well-being and mental health), customers, suppliers and our communities	●	●	●	●	●	●	●
Managing demands on or expectations of workforce to work remotely or as part of a hybrid work environment	●	●	●	●	●	●	●
Rising threat of catastrophic natural disasters and weather phenomena	●	●	●	●	●	●	●
Enhanced exposure to fraud in the industry	●	●	●	●	●	●	●
Uncertainty surrounding core supply chain ecosystem	●	●	●	●	●	●	●

2024 risk concerns

Figure 20 reveals that respondents from five of the seven industry groups perceive that the magnitude and severity of risks in the overall environment affecting their organisation will decrease in 2024 from the 2023 levels, with six industry groups indicating that they will be above 2022 levels. When comparing the number of risks appearing in both the 2024 and 2023 surveys that are rated at the "Significant Impact" level, there is a noticeable decrease in the collective number of risks at that level across all industries for 2024 compared to 2023. For 2024, three macroeconomic risks are rated by one or more industries at the "Significant Impact" level, compared to six macroeconomic risks at that level for 2023. For strategic risks, the decrease in the number of risks rated at the "Significant Impact" level dropped from five in 2023 to one in 2024. The decrease in number of "Significant Impact" risks for operational risks is from 10 in 2023 to four 2024 risks.

Respondents in the Healthcare industry group rate the most risks at the "Significant Impact" level, with seven for 2024. Four of their seven highest-rated risks are operational in nature, with concerns related to cyber threats, data privacy, third-party risks and talent shortages (most likely clinical healthcare workers, particularly nurses). Financial services respondents rate four of the 36 risks at the "Significant Impact" level, with two of those four relating to overall economic conditions and the current interest rate environment (both macroeconomic issues), one related to heightened regulatory scrutiny, and one related to cyber threats. Only two other industry groups rate at least one risk at the "Significant Impact" level. The Consumer Products and Services industry group rates the macroeconomic risk related to economic conditions and inflationary pressures at the "Significant Impact" level and the Technology, Media and Telecommunications industry group rates cyber threats at that level of significance.

Three of the seven industry groups rate cyber threats as a "Significant Impact" risk: Financial Services; Technology, Media and Telecommunications; and Healthcare. The Financial Services, Consumer Products and Services, and Healthcare industry groups are all concerned about economic conditions, including inflationary pressures. Financial Services and Healthcare are the two industry groups also most concerned about heightened regulatory scrutiny.

With the continuing transitions happening in energy generation, it is not surprising that Energy and Utilities respondents believe that 2024 will be riskier than 2023, even though none of the 36 risks they rate is at the "Significant Impact" level. In addition, Energy and Utilities respondents rate 10 of the 36 risks as "Less Significant Impact" (4.50 or lower), more than any other industry group.

All industry groups rate cyber threats as a top five risk concern, suggesting no industry is immune to those exposures. All industry groups, except Energy and Utilities and Government, include concerns about economic conditions, including inflationary pressures, as a top five risk concern. And all industry groups, except Financial Services, highlight concerns about the ability to attract, develop and retain talent as a top five risk concern for 2024. Increases in labour costs are of particular concern for Healthcare, Consumer Products and Services, and Government for 2024.

2034 risk issues

The significance of risk concerns a decade out is noticeably higher than short-term risk concerns. For five of the seven industry groups, all of the top five risks for 2034 are at the "Significant Impact" level. This is in contrast to 2024, where only one industry group (Healthcare) rated all top five risks at that level. The Healthcare industry group rates one of its risks at noticeably high levels (exceeding 7.0) for 2034. It also rates the long-term outlook as higher than how it viewed the 10-year outlook last year, suggesting its long-term risk perceptions have elevated from last year. Government entities also view long-term risks as more significant than their view of those risks last year, with four of their top five risks rated higher for 2034 than 2033.

TABLE 13

Perceived impact for 2024 and 2034 — by industry group

Macroeconomic Risk Issues	Year	FS	CPS	MD	TMT	HC	EU	GOVT
Economic conditions, including inflationary pressures	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Increases in labour costs	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Change in current interest rate environment	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Adoption of digital technologies requiring new skills in short supply	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Access to capital/liquidity	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Impact of social issues and DEI priorities on ability to attract/retain talent and compete	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Geopolitical shifts, regional conflicts and instability in governmental regimes or expansion of global terrorism	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●

Macroeconomic Risk Issues (continued)	Year	FS	CPS	MD	TMT	HC	EU	GOVT
Volatility in global financial markets and currency exchange rates	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Changes in global markets and trade policies	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Pandemic-related government policies and regulation	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●

Strategic Risk Issues	Year	FS	CPS	MD	TMT	HC	EU	GOVT
Heightened regulatory changes and scrutiny	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Organisation not sufficiently resilient and/or agile to manage an unexpected crisis	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Limited opportunities for organic growth	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●

Strategic Risk Issues (continued)	Year	FS	CPS	MD	TMT	HC	EU	GOVT
Sustaining customer loyalty and retention	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Formulating business response to legal, political and social issues that are polarising	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Social media developments and platform technology innovations	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Growing focus on climate change and other sustainability policies, regulations, and expanding disclosure requirements as well as expectations of key stakeholders	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Ease of entrance of new competitors or other changes in competitive environment	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Difficulty in growing through acquisitions, joint ventures and other activities	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Substitute products and services that affect the viability of our business	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Performance shortfalls that trigger activist shareholders	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●

Operational Risk Issues	Year	FS	CPS	MD	TMT	HC	EU	GOVT
Cyber threats	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Ability to attract, develop and retain top talent, manage shifts in labour expectations, and address succession challenges	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Third-party risks	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Ensuring privacy and compliance with growing identity protection expectations	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Challenges in sustaining culture due to changes in overall work environment	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Existing operations and legacy IT infrastructure unable to meet performance expectations as well as "born digital" competitors	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Inability to utilise rigorous data analytics to achieve market intelligence and increase productivity and efficiency	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Resistance to change restricting organisation from adjusting business model and core operations	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●

Operational Risk Issues (continued)	Year	FS	CPS	MD	TMT	HC	EU	GOVT
Organisation's culture not sufficiently encouraging timely identification and escalation of emerging risk issues	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Meeting expectations around protecting health and safety of employees (including their well-being and mental health), customers, suppliers and our communities	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Managing demands on or expectations of workforce to work remotely or as part of a hybrid work environment	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Rising threat of catastrophic natural disasters and weather phenomena	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Enhanced exposure to fraud in the industry	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●
Uncertainty surrounding core supply chain ecosystem	2024	●	●	●	●	●	●	●
	2034	●	●	●	●	●	●	●

Figures 21-27 on the following pages summarise the top-rated risks by industry group separately for 2024 and 2034. Only the top five risks are reported and, where available, scores for 2023 and 2022 (for comparisons to 2024) and 2033 and 2032 (for comparisons to 2034) are also provided.

Cyber threats are in the top five long-term risks for all industry groups. And concerns about attracting, developing and retaining top talent, including succession challenges, are in the top five risks for all industry groups. Four of seven industry groups are concerned about heightened regulatory changes and scrutiny. That is the number one long-term concern for Energy and Utilities organisations.

The rising threat of catastrophic natural disasters and weather phenomena is a top five long-term risk concern for Energy and Utilities and Government Agencies. The Energy and Utilities industry group is the only group to rate concerns surrounding a growing focus on climate change and other sustainability policies as a top five risk.

These noted differences in perceptions of risk issues across the different industry groups highlight the importance of understanding industry drivers and emerging developments in order to identify the most significant enterprise risks and emerging risk concerns in each group.

Following each set of bar charts by industry group, we provide additional commentary about industry-specific risk drivers.

Noted differences in perceptions of risk issues across the different industry groups highlight the importance of understanding industry drivers and emerging developments in order to identify the most significant enterprise risks and emerging risk concerns in each group.

FIGURE 21A

Financial Services — 2024

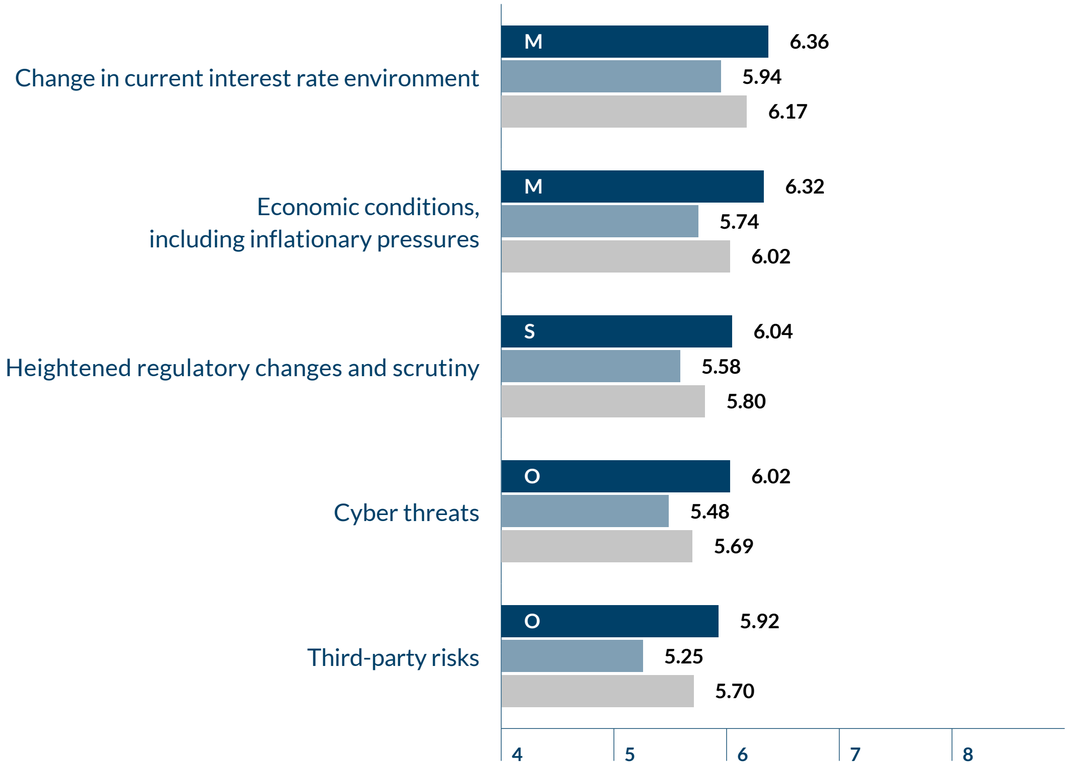
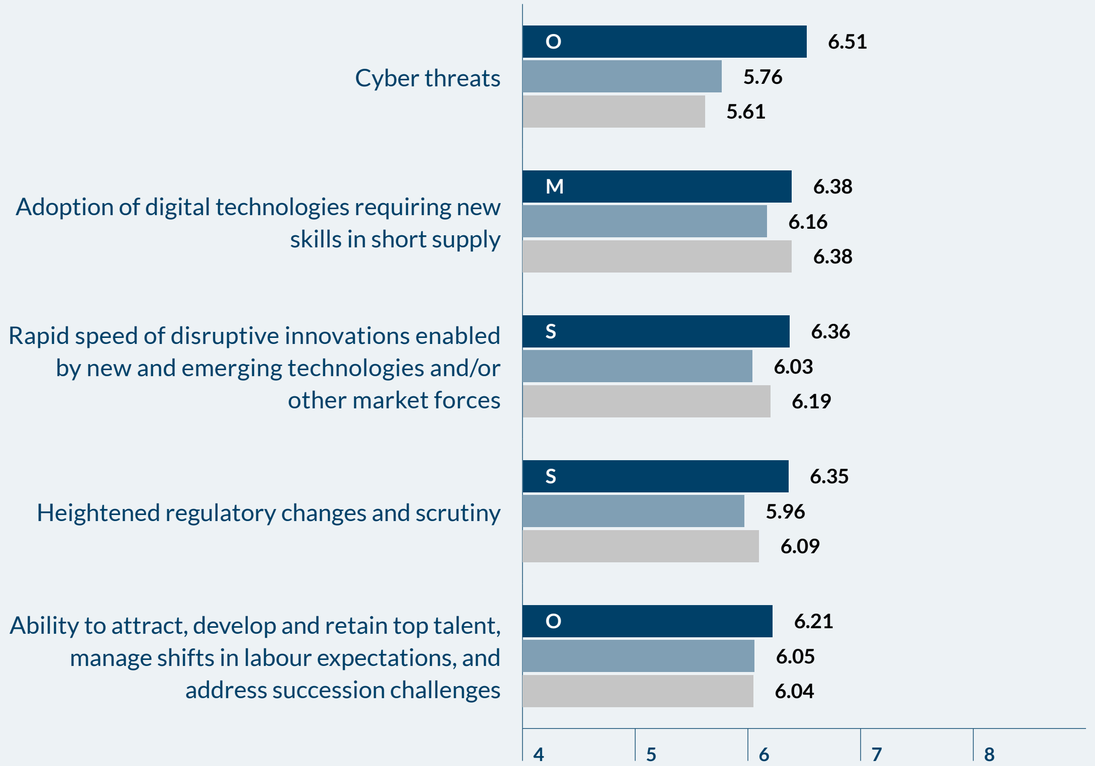


FIGURE 21B

Financial Services — 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.

Commentary — Financial Services Industry Group

BY MICHAEL BRAUNEIS
GLOBAL LEADER, FINANCIAL SERVICES INDUSTRY PRACTICE, PROTIVITI

Protiviti and NC State University's ERM Initiative have been conducting our Top Risks Survey for the past 12 years. This journey began just as financial markets around the world were starting their long, slow recovery from the global financial crisis, and has since covered the worst global pandemic in 100 years as well as near record-low interest rates followed shortly by the fastest rate hiking cycle in history.

In this context, getting the first look at each year's survey results and comparing them to the prior year's is always interesting — but the most compelling years to analyse are those in which the market breaks from recent trends and gives us some new risks to talk about. It's safe to say that 2024 is one of those years.

Our observations

Executives have arrived at a pessimistic consensus. Our 2023 survey results reflected a deep sense of uncertainty and ambiguity, with many executives concerned that a recession was imminent even as they struggled to attract and retain staff in a red-hot job market. We commented in our 2023 report that we were surprised that the risk tied to economic conditions and inflation dropped from second place in 2022 to third in 2023, as we saw financial markets facing increasing headwinds. Fast-forwarding to the results for 2024, the liquidity crisis and resulting bank failures in early 2023, a tougher regulatory environment and push to raise capital, higher funding costs, and expectations of having to manage the business in a "higher for longer" interest rate environment have collectively convinced financial services leaders that the industry is indeed in a tougher economic cycle. Interestingly though, concerns about access to capital and liquidity only ranked 16th on the list of top risks, up slightly from 20th place last year. This suggests our respondents are more concerned about the impact that current market conditions are having on their profitability and growth prospects than as a threat to their survival.

Partially as a result, the war for talent is abating. In last year's survey summary, we predicted that concerns about talent would diminish by the time of our 2024 survey and that turned out to be an accurate forecast. Considering the economic challenges above, financial institutions have cut spending significantly and many have put hiring freezes in place. While there is still significant competition for talent in pockets — notably in data, AI/machine learning, and regulatory compliance — overall, voluntary attrition rates in the United States have come down significantly according to data from the Bureau of Labour Statistics,[6] and compensation expectations are normalising. As a result, concerns about attracting and retaining talent saw a big drop in this year's survey results, from second to sixth place.

The liquidity crisis and resulting bank failures in early 2023, a tougher regulatory environment and push to raise capital, higher funding costs, and expectations of having to manage the business in a "higher for longer" interest rate environment have collectively convinced financial services leaders that the industry is indeed in a tougher economic cycle.

[6] "Job Openings and Labor Turnover — September 2023," News release from the Bureau of Labor Statistics, November 1, 2023: www.bls.gov/news.release/pdf/jolts.pdf.

In general, financial services leaders feel we are in a riskier time. In addition to the risk ranking order, it's also instructive to look at the average scores assigned to the top risks and how those have changed year over year. We look at this as our survey's version of a VIX score or "fear gauge." In 2023, the top risk (change in interest rate environment) received an average 5.94 score on our 10-point scale. In 2024, interest rates remained the top risk but the score for that factor increased to 6.36. The average score of the top five risks as a group in 2024 rose to 6.13 from 5.76 in 2023. Maybe most notably, the top four risks in 2024 all earned a higher score than the top risk in 2023 did. In other words, although several of the top concerns from last year remain near the top of the list this year, the level of concern has gone up across the board.

Unsurprisingly, cyber risks took a big jump — and are likely to grow further. Last year, we were surprised that cyber threats only ranked as the 11th highest risk, particularly as this was the top risk for 2022. For 2024, this trend has reversed and cyber risk has moved back into the top five. Notably, our 2024 results were collected before the high profile ICBC ransomware incident occurred in November, which is causing financial institutions around the world to reevaluate both their own cyber risk management controls as well as how they would address threats that impact their critical counterparties. As a result, we wouldn't be surprised to see this risk move even higher on the list for 2025.

An increasingly complex third-party risk landscape drove that item up the list. Third-party risk took the largest leap of all items on our list in 2024, rising 11 spots to fifth. We believe there are multiple factors behind this, including:

- Growing concerns about counterparty credit risk and financial stability driven by the economic conditions described above;
- An ever-larger list of security breaches caused by third-party vendors and/or technology platforms they provide;
- Growing reliance on cloud and software-as-a-service providers across the financial services industry; and
- Increasing regulatory scrutiny related to third-party partnerships, particularly at the intersection of banking and fintech where banking regulators have criticised insured depository institutions serving as a conduit for less regulated fintechs without appropriate review and oversight of their activities by the bank.

While concerns about the economy and the regulatory response dominate the top of the list, technological innovation and related infrastructure needs follow closely behind. "Existing operations and legacy IT infrastructure unable to meet performance expectations as well as 'born digital' competitors," "adoption of digital technologies requiring new skills in short supply," and "inability to utilise rigorous data analytics to achieve market intelligence and increase productivity and efficiency" all appear among the top 10 risks for the third year in a row. This presents a critical strategic challenge as financial institutions attempt to cut expenses aggressively even as the cost of technology modernisation efforts continues to rise — and executives recognise that the only thing worse than incurring these costs is not making the investment and falling further behind more innovative competitors. This dynamic will put significant pressure to cut costs even further in other areas as technology consumes an ever-greater share of operating expenses in the financial services industry.

Looking ahead to 2034

For the past few annual surveys, we've also asked respondents about the top risks they expect to face 10 years in the future. For our respondents, the 2034 view generally mirrors the decade-out results we received last year, with a few exceptions that seem to be coloured by a focus on 2024's top risks.

Consistent with our prior year results, concerns about keeping up with the threat of digital disruption continue to dominate the longer-term view. Cyber threats jumped and worries about attracting talent dipped a bit, which is consistent with the trend described above regarding 2023 vs. 2024 results.

Other noteworthy results in the 2034 review:

- Regulatory scrutiny remains high on the list both in the current and 10 years' out view, and this has been the case for as long as we have conducted this survey. This is interesting given the exciting innovations coming online for compliance functions, particularly involving data analytics and generative AI. We think these will become truly groundbreaking advancements that will finally allow financial institutions to get ahead of regulatory expectations in key areas like financial crimes while bending the cost curve down over time. Is the market more pessimistic than we are about the opportunities that exist in this area, or does it simply believe that lawmakers and regulatory agencies will continue to move the bar just out of reach?

- "Change in current interest rate environment" jumped from 14th on last year's 10-year outlook list to seventh in 2034. Is this just recency bias given the impact the rate environment has had in 2022 and 2023, or do our respondents think that rate trends will move higher in the foreseeable future? What we also found interesting is that historically, moderately higher rates are good for financial institutions' margins — with most of the current stress being caused by short-term funding costs increasing while the value of long-dated assets has fallen. This is a temporary problem that will diminish as longer-term assets that were priced during times of record-low rates run off. Perhaps concerns that higher-for-longer interest rates will constrain funding demands and deal flow are outweighing the margin upside that this scenario would represent for our respondents.

- Finally, there are a few 2034 risks that fell closer to the bottom of the list than we would have expected:

  – "Geopolitical shifts, regional conflicts and instability in governmental regimes or expansion of global terrorism" moved up five spots from last year but is still only in 25th place, and "changes in global markets and trade policies" held steady at 33rd place, making it the fourth lowest-rated risk. These results are surprising in light of growing geopolitical conflicts from the Russian/Ukraine war, regional tensions in the Pacific, and renewed fighting between Israeli and Palestinians and heightened risk of broader conflicts in the Middle East as a result. Of note, we did see a notable increase in risk ratings provided by respondents who completed our survey after the October 7, 2023, events in the Middle East.

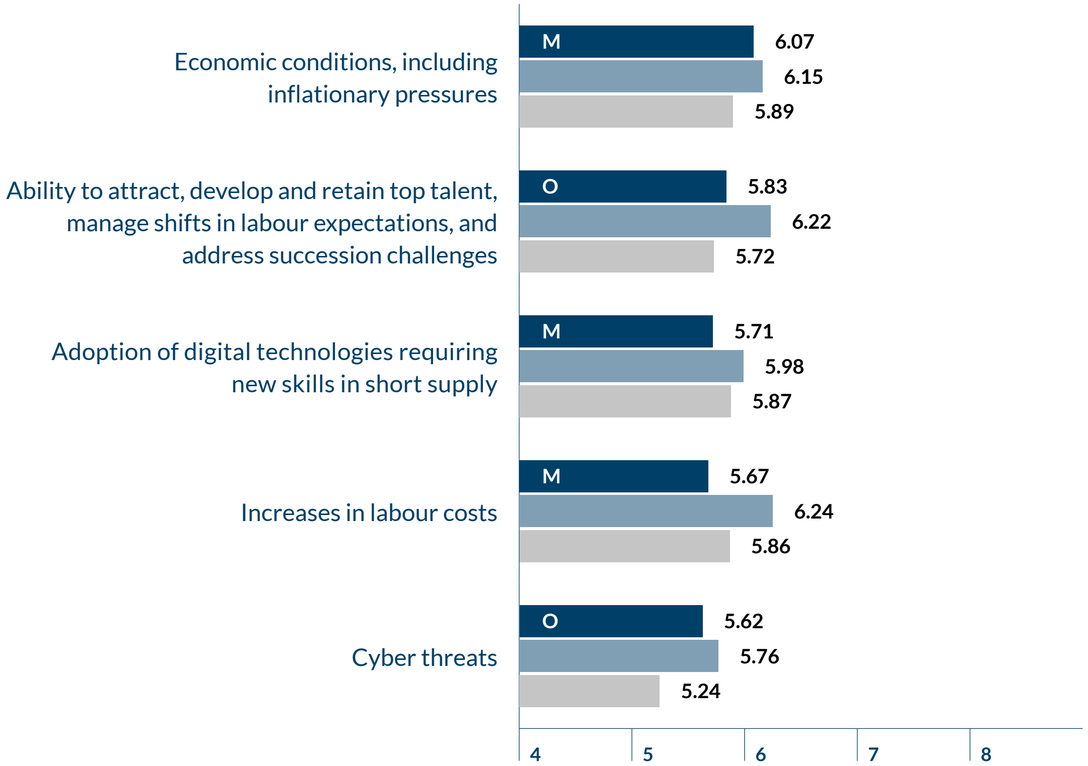
  – "Formulating business response to legal, political and social issues that are polarising" was a new addition to our survey this year but only came in at 29th place. Likewise, "impact of social issues and DEI priorities on ability to attract/retain talent and compete" actually dropped from 24th to 30th place this year. Given that both issues have continued to consume a greater share of business leaders' attention as well as media scrutiny regarding their companies over the past year, it's interesting that our respondents think they will be so much less significant as concerns a decade out.

  – Lastly, "managing demands on or expectations of workforce to work remotely or as part of a hybrid work environment" dropped nine spots from 22nd to 31st place. While we've certainly seen progress over the past 12 months in financial institutions bringing a larger share of their workforces back into the office, overall attendance rates vary significantly by geography and many financial institutions have told us that they are still not consistently where they would like to be in this regard. Our survey results suggest the market believes these challenges will be fully resolved, though, and that a significant percentage of remote or hybrid work is not part of the long-term future of financial services.

Regulatory scrutiny remains high on the list both in the current and 10 years' out view, and this has been the case for as long as we have conducted this survey. This is interesting given the exciting innovations coming online for compliance functions, particularly involving data analytics and generative AI.

FIGURE 22A

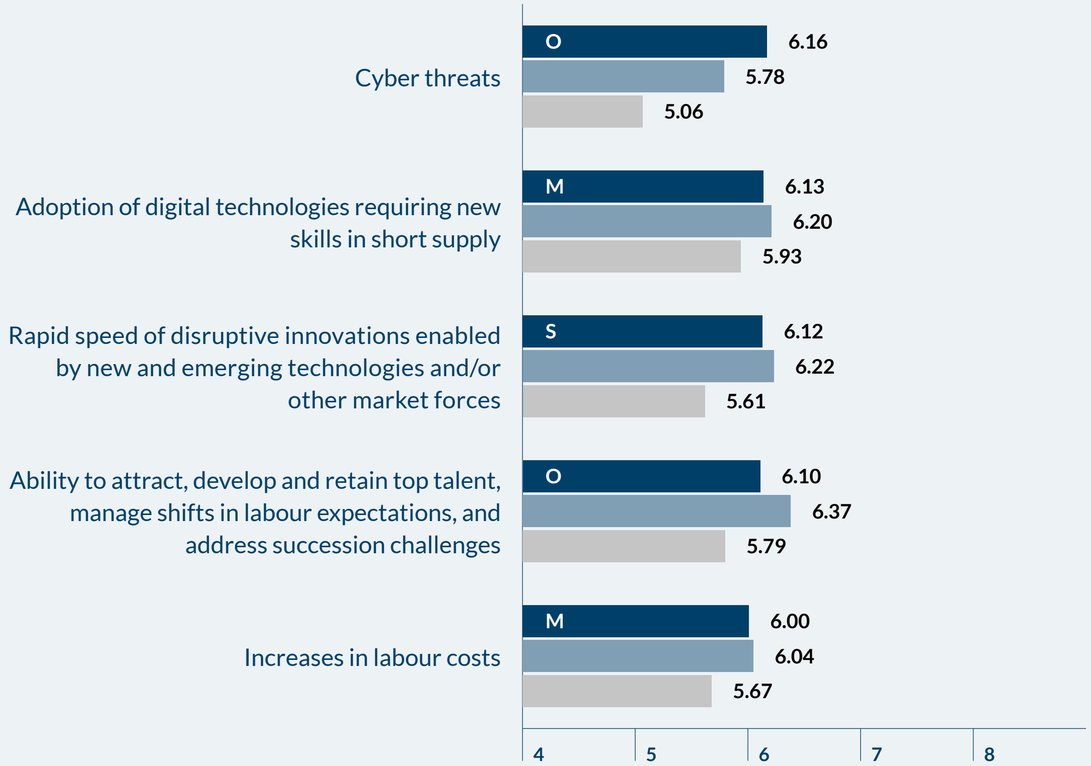
Consumer Products and Services — 2024



M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue 2024 2023 2022

FIGURE 22B

Consumer Products and Services — 2034



M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue 2034 2033* 2032*

* 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.

Commentary — Consumer Products and Services Industry Group

BY CAROL RAIMO
GLOBAL LEADER, CONSUMER PRODUCTS AND SERVICES INDUSTRY PRACTICE, PROTIVITI

The Consumer Products and Services industry group faces a long list of headwinds heading into 2024. Inflationary pressure, workforce attrition with talent gaps and protecting customers' data are top on the list of major concerns weighing on the minds of senior executives in the consumer packaged goods (CPG) and retail industry group. Separately, for hospitality and airlines companies, cyber threats, the rising threat of catastrophic natural disasters, and geopolitical shifts and regional conflicts are cited among these industries' top risks.

In Protiviti's latest Top Risks Survey, CPG and retail executives were asked to provide their perspectives on the biggest risks facing their organisations over the next 12 months and a decade ahead. Their views reflect a growing sense of uncertainty in today's business environment, where market competition remains fierce, the costs of goods and labour continue to rise, and companies are desperate for new technologies to better manage risks and improve customer experience.

Even as supply challenges have normalised, the difficult macroeconomic environment has made it challenging for CPG and retail companies to forecast future demand and make growth plans. Industry leaders are exploring ways to retain and grow their customer base with customer loyalty programs and new payment strategies for shoppers.

But how can you pass on the high cost related to inflation and supply chain disruptions to customers without hurting customer satisfaction and loyalty? How do you retain your top talent and keep a lid on rising labour costs? These are tough questions that business leaders must tackle head on, and they can only do this effectively with access to data analytics and market intelligence, which consequently, is identified as the ninth-rated risk for 2024 by CPG and retail executives who responded to the survey.

Below we discuss other top risks identified by CPG and retail respondents.

The difficult macroeconomic environment has made it challenging for CPG and retail companies to forecast future demand and make growth plans.

Macroeconomic and labour market challenges

Few industries have been more impacted by inflation than the CPG industry so it is no surprise that executives cited economic challenges, including inflation, as their No. 1 risk for 2024, with workforce-related challenges coming in at second place.

A change in the interest rate environment is another source of concern. Since 2022, the Federal Reserve's campaign to fight inflation by increasing interest rates has hurt companies' ability to borrow and grow. Although rate increases have slowed this year, business leaders fear the Fed might not reverse course next year if inflation remains high. CPG and retail respondents cited the interest rate issue as the No. 7 risk for 2024.

On the labour front, the CPG and retail industry are experiencing a perfect storm as workers leave in search of a better work-life balance, greater incentives (salary and benefits), flexibility, and a working environment that better supports their mental health and overall well-being. The labour issues and economic fears are clearly interconnected. In the United States, the CPG industry provides 2.3 million jobs and the retail industry, the largest private-sector employer in the U.S., supports 52 million jobs. Although the labour market has remained resilient, job growth is expected to decelerate in the coming months

in lockstep with slower economic activity and the prospect of restrictive credit conditions, according to the National Retail Federation.

To address the workforce challenges and transform their relationship with employees, retail business leaders must develop a deeper understanding of the labour dynamic and the forces driving changes across the industry. The conversation should begin in the boardrooms and executive suites, starting with these prompting questions: What do frontline employees and managers want in a job? What will motivate them to show up every day?

The customer should be front and centre in the inflation discussion. In particular, as household debt, especially credit card debt, hits an all-time high, brands and retailers need to consider the impact of a stressed consumer and higher interest rates on consumer behaviour. They also need to consider which parts of their customer base are more and less impacted by inflation, so they can adjust their marketing and advertising strategies accordingly.

Cost optimisation through automation and technology modernisation

The economic uncertainty and inflationary pressures are also forcing CPG and retail companies to explore different ways to cut costs. It's a sink-or-swim situation for many, especially smaller companies that have limited purchasing power and ability to negotiate lower cost with suppliers. With margins compressing, companies are reassessing working capital and cash flow management, reducing inventory in warehouses and negotiating pricing with suppliers, among other cost optimisation measures.

Visibility and transparency into data are crucial for making informed cost-cutting decisions, and so companies also are investing time and resources into automation to improve operational efficiencies and data analytics to gain better visibility into all aspects of operations.

AI and other technology tools are becoming increasingly important as companies consider running their businesses with fewer people.

Legacy systems, however, are proving to be a challenge; automation is easier for current technologies, but more difficult for legacy ones. As a result, the retail and CPG executives who participated in the survey said they are particularly concerned about the inability of existing operations and legacy IT infrastructure to meet performance expectations as well as "born digital" competitors. This concern was ranked fifth among the 2024 top risk issues.

Additionally, the respondents said they are worried about the ability of their organisations to adopt digital technologies given the shortage in technical staff (ranked 10th for 2024). Despite these concerns, some retail and CPG companies are being aggressive in adopting new technologies. A separate survey conducted by Protiviti recently found that more than half of financial executives in the retail and CPG industry are already deploying generative AI to predict consumer behaviours, suggest timely product recommendations, optimise pricing, mitigate fraud and manage inventory.

AI technologies are becoming increasingly important as companies seek to stay ahead of the competition, run their businesses with fewer people and enhance customer experience. The challenge for some companies will be finding the most efficient way to integrate these technologies into existing legacy systems without hurting productivity or introducing new risks, such as cyber attacks.

Cybersecurity and data privacy expectations

Ensuring privacy and compliance with growing identity protection expectations has become a C-suite priority in today's omnichannel environment. Previously, companies relied on third parties to collect and sell consumer data,

but now they are keeping it in-house. This shift in data ownership requires them to prioritise data protection.

At the same time, as more retail and CPG companies transform digitally, the threat of cyber intrusion or operational failures that result in data exposures has risen dramatically. Recent industry-related cyber attacks have included digital disruptions to production lines and supply chains. The concerns about cybersecurity are evident from the recent SEC guidance on cybersecurity disclosures, which focus on protecting information and assessing its impact on organisations.

As cyberattacks continue to increase in severity, CPG and retail organisations need to prioritise protection and compliance. It also means paying attention to third-party risks, which could emanate from IT vendors and/or supply chain partners. Organisations that fail to prioritise these issues face executive fallout and brand reputation risk.

Sustaining customer loyalty

The future of customer loyalty and buying patterns remains uncertain. Consequently, CPG and retail respondents rated sustaining customer loyalty and retention as the sixth-ranked risk for 2024. The abundance of options and channels to connect with consumers is among the reasons why companies find it harder to maintain customer loyalty. Loyalty between brands and consumers is being tested as mergers and acquisitions disrupt the marketplace.

Still, customer experience needs to be a focal point and an important battleground for brands to consider. Great products and services are no longer enough; the consumer's experience with purchasing and utilising the product or service has to be a priority as well. Brands should make decisions with the mindset that they cannot prioritise their own interests over customer satisfaction.

The big picture: Looking a decade ahead

Due to the current challenging business environment, many CPG and retail organisations are primarily focused on maintenance work rather than funding transformational programs. This lack of forward investment and focus on routine operations are likely to continue until there is more clarity and confidence in the business environment.

Like in previous years, CPG and retail respondents were asked to look into their crystal ball and identify risk issues they expect over the next decade. The ability to attract, develop and retain top talent, manage shifts in labour expectations, and address succession challenges came in at No. 1, followed by the rapid speed of disruptive innovations, and sustaining customer loyalty and retention.

Customer experience needs to be a focal point, and brands should make decisions with the mindset of improving the customer experience continuously.

Hospitality Industry

The industry is slated to record its best year ever in 2023, a reflection of its resilience in the face of major headwinds and years of setbacks. Still, industry leaders are concerned about several major risks heading into the new year, including a potential return of effects of the pandemic.

Cyber threats is top on the list of risks for hospitality executives. This is no surprise. In recent months, there has been a rise in reported cyberattacks using malware in the gaming industry. The liability exposure and reputational risk here are significant because the gaming industry collects a vast amount of personal data and preference information from its guests, making it a prime target for cyberattacks.

In addition to the cyber threats, the hospitality respondents identified the rising threat of catastrophic natural disasters and pandemic-related government policies and regulations as their top three risks for 2024. Rising labour costs and adoption of digital technologies requiring new skills round out the top five.

In recent years, the lodging industry (e.g., hotels, motels, resorts, timeshares) has been focused on updating their technology infrastructure, especially guest-facing technology, which is important for enhancing guest experiences and streamlining processes. Interactive gaming and online gaming providers are also driving the development of new systems and infrastructure.

Clearly, the industry is still mindful of the impact of the pandemic and its lingering effects. The cruise line segment, for example, experienced significant losses during the pandemic and is now navigating the uncertainties of potential future disruptions. Given the pandemic experience, it makes sense that executives fear that a turn of events, such as a COVID variant or a decline in consumer confidence, could have a material impact on the industry's recovery.

The worry over natural disasters makes sense given the location of properties and the fact that safety and security of guests and employees is always a top priority for the industry. It may also be related to increased focus on ESG, and consumer expectations around the "E" in ESG or environmental responsibilities.

The high labour cost is both a reflection of inflation and the effects of the exodus of workers in the wake of the pandemic. According to the Journal of Hospitality and Tourism Management, the hospitality industry lost more than 8.2 million jobs between February and April of 2020, making it the hardest-hit industry in the United States.

Airline Industry

Airline executives cited increased labour costs, geopolitical shifts and regional conflicts, and economic conditions, including inflation, as their top 3 risks issues for 2024. Like hospitality, the airline industry is expected to return to profitability this year after several years of disappointing financial performance.

But even with the strong recovery, the industry is keeping a close eye on the macroeconomic picture, which continues to create a lot of uncertainty. For the industry, higher costs relating to energy prices and labour, and an escalation in geopolitical events, are big risks that could reverse the already fragile gains made toward profitability.

FIGURE 23A

Manufacturing and Distribution — 2024

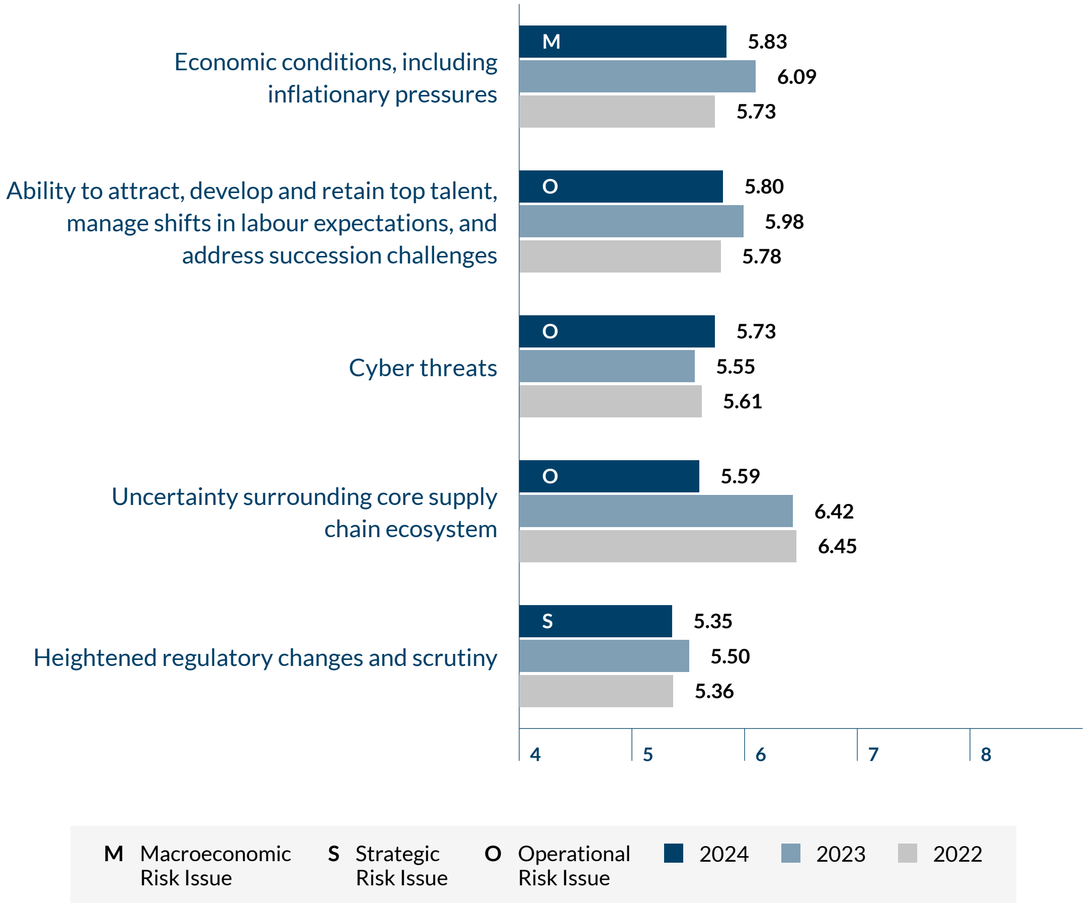
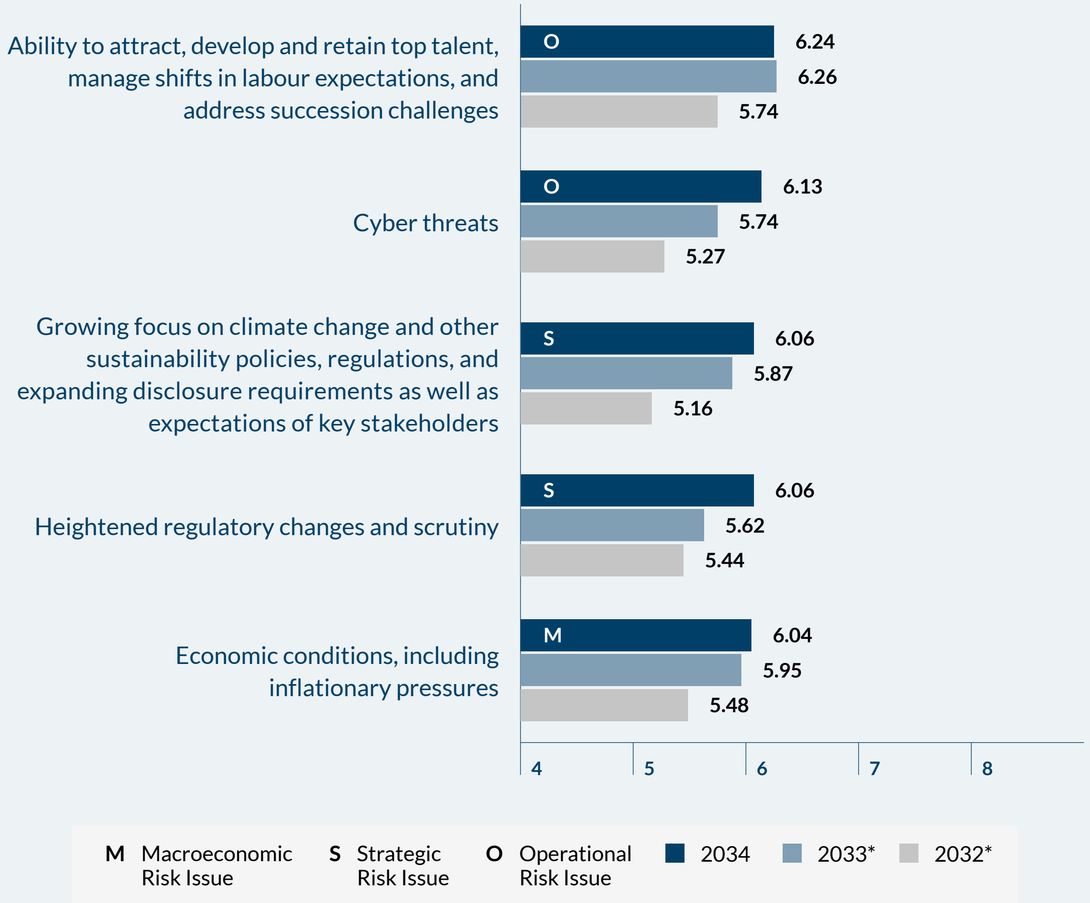


FIGURE 23B

Manufacturing and Distribution — 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.

Commentary — Manufacturing and Distribution Industry Group

BY SHARON LINDSTROM
GLOBAL LEADER, MANUFACTURING AND DISTRIBUTION INDUSTRY PRACTICE, PROTIVITI

In an ever-evolving and rapidly changing business landscape for manufacturing and distribution organisations, executives and boards are challenged to navigate myriad risks, particularly as their businesses continue to play catch-up on numerous fronts in areas such as innovation and digital transformation. The risks these organisations face, both short- and long-term in nature, represent a complex array of external and internal factors ranging from talent management, cyber threats and supply chain dynamics to economic and inflationary concerns, regulatory changes and scrutiny, and technological advancements.

Overview of top risk issues in 2024

For the coming year, economic conditions, including inflationary pressures, represent the most significant risk for manufacturing and distribution organisations. Despite positive trends in demand and production over the past several months, the looming spectre of inflation remains a concern amid broader global uncertainty. Of note, the Manufacturing Purchasing Managers' Index (PMI) has been showing an uptick in recent months, indicating a positive trajectory, but the industry understandably remains cautious. Notably, this concern is expected to decrease in significance over the next decade, dropping to the fifth position in terms of long-term risks for 2034.

A growing number of bad attackers see manufacturing OT environments as opportunities to execute ransomware attacks on these organisations, increasing their cyber risk profiles even more.

The challenge of attracting, developing and retaining top talent remains high on the list of risks manufacturing and distribution organisations face — an ongoing situation compounded by shifts in expectations among workers as well as succession challenges. Skills shortages continue to fuel low unemployment rates (in the range of 3%) throughout the industry. Specific manufacturing-heavy regions also continue to experience scarce talent availability — a persistent issue for organisations that have locations in more non-urban areas, making it difficult to compete with job opportunities in more popular urban areas.

In a related finding, rising labour costs appear to be of less concern, having dropped in importance on the list of top risks for the industry group. Further, the decline is more pronounced than in other survey results, indicating a shift in the industry's focus from labour cost concerns to broader challenges such as talent management, cybersecurity and supply chain resilience.

Similar to most other industries, cyber threats have resurfaced as a top concern for manufacturing and distribution organisations, likely due to perceived vulnerabilities in operational technology (OT) systems as well as the proliferation of IoT-connected devices and technologies within industrial environments. Manufacturers historically have not been viewed as prime targets for cyber attacks. Consequently, vulnerability management has not been a focus in the same way that it has for organisations in other industries (for example, financial services and retail). However, a growing number of bad actors see manufacturing environments as opportunities to execute ransomware attacks because they can be deployed in industrial environments that tend to be older and run on limited hardware that lacks readily available protections, such as anti-malware, anti-virus and on-device monitoring solutions. This increases the industry's cyber risk profiles even more.

Additionally, manufacturers that produce IoT-connected goods must ensure the security of their products to their markets to minimise brand and reputation risk of a breach.

Another key point: New SEC-required cyber disclosures have elevated the importance of cybersecurity for publicly held companies in the industry, bringing added attention to the potential disruption of production processes.

Concerning supply chain risks, the uncertainty surrounding the core supply chain ecosystem has shifted from being the top concern in recent years to the fourth position for 2024. Factors contributing to this change include the industry's recovery from severe pandemic-related supply chain disruptions, significantly lower shipping costs globally relative to the height of the pandemic, and greater investments in building supply chain resiliency and innovation. These are positive outcomes based on lessons learned in the pandemic era. Despite the moderation in perceived risk level, however, supply chain dynamics remain a significant risk, and organisations must continue to adapt to ongoing challenges, especially as the global business and geopolitical landscape continues to shift.

The manufacturing and distribution industry also faces heightened regulatory changes and scrutiny (the fifth-ranked risk issue for 2024), with increased focus on ESG regulations and disclosure requirements, including cybersecurity, as noted earlier. Among the more notable new ESG requirements is the Corporate Sustainability Reporting Directive, which requires new, standardised and detailed sustainability reporting by companies operating in the European Union. This shift aligns with global trends and expectations for companies to operate sustainably and transparently. Among the challenges for manufacturing and distribution organisations is navigating these complex regulatory landscapes while maintaining operational efficiency.

Though not in the top five for the Manufacturing and Distribution industry group, other risk issues that landed in the top 10 are worth noting. An inability to leverage rigorous data analytics for market intelligence and increased productivity ranks sixth. This is understandable considering that many organisations in the industry group must manage disaggregated and decentralised data sets, along with older, legacy technology systems (making technical debt another challenge). As a result, extracting valuable, meaningful insights from this data presents a significant hurdle.

Another notable risk issue for 2024 is the adoption of digital technologies requiring new skills that are in short supply. This risk presents challenges on several fronts. New technologies have brought about transformative benefits for manufacturing and distribution companies in terms of operational efficiency and financial performance. However, this paradigm shift also necessitates unique skillsets that, as noted earlier, are in short supply. This challenge is particularly acute for these companies because, on average, they tend to lag behind other sectors in the adoption of new technologies and innovations. In addition, as manufacturing and distribution organisations seek to expand their digital transformation efforts, they must navigate an increasingly complex ecosystem of partners. Moving to cloud-based solutions and integrating more technology into operations prompts greater reliance on third parties. While these changes bring strategic advantages, they also call for comprehensive risk management.

Geopolitical risks are another pressing concern. Current global events are exacerbating geopolitical uncertainties with regional conflicts and instability in governmental regimes or expansion of global terrorism complicating the risk landscape for manufacturing and distribution organisations with international operations. The interconnected nature of their supply chains means that political instability has far-reaching implications.

Interestingly, and consistent with results for other groups analysed in our survey, resistance to change drops on the 2024 list of top risks for manufacturing and distribution organisations, rounding out the top 10. However, given the volatility in the business environment and technology-driven transformation underway in many companies

(e.g., Industry 4.0), it's imperative for leaders in these organisations to continue monitoring workplace culture to ensure teams are open to and embracing the use of emerging technologies and new ways of working.

Overview of top risk issues in 2034

Looking ahead to 2034, talent management emerges as the top risk issue, mirroring current trends but projected to grow over the next decade. The challenge lies not only in attracting, developing and retaining top talent, but also in managing shifting worker expectations and addressing succession challenges against demographic changes, perception issues around manufacturing jobs' desirability compared to other sectors like retail or services, the aforementioned location of available jobs in more rural and remote locations globally, and evolving skill requirements resulting from technological advancements and ongoing transformation initiatives.

Over the next decade (and as is the case for most other industries), cyber threats are expected to increase for manufacturing and distribution organisations, necessitating a dual focus on OT security and IoT devices — both those used in manufacturing facilities as well as those produced and distributed by manufacturers. The increased connectivity brought about by Industry 4.0 creates more entry points for cyberattacks, while the emergence of sophisticated attacks and lack of preparedness heightens the risk. These threats will only grow long-term as technological advances fuel greater capabilities among bad actors to attack and penetrate organisations' technology systems. Cybercriminals already are becoming more sophisticated in targeting intellectual property and sensitive commercial data, as well as disrupting production lines — all of which carry serious financial ramifications.

The global focus on climate change and sustainability is expected to become a paramount concern for manufacturing and distribution organisations over the long term. The industry increasingly is coming under the spotlight as global efforts to combat climate change intensify. Particularly within energy-intensive sectors such as materials (cement, iron and steel) and chemicals, the responsibility for reducing carbon emissions is becoming significant.

Over time, manufacturing and distribution organisations expect to face greater scrutiny and potentially more climate-related regulations. This is one factor driving the high ranking of heightened regulatory changes and scrutiny in the 2034 risk outlook. As noted earlier, an evolving landscape of ESG regulations and increased disclosure requirements adds further complexity to the compliance efforts most manufacturers and distributors are undertaking. These organisations must navigate this intricate regulatory environment while ensuring their operations align with sustainability goals.

A number of technology-related concerns permeate the top 10 long-term risk issues for the industry group, including the adoption of digital technologies requiring new skills in short supply, the rapid speed of disruptive innovations, and existing operations and legacy IT infrastructure unable to meet performance expectations as well as "born digital" competitors. These challenges underscore the gap board members and executives in the industry may perceive with regard to how their organisations are planning for and incorporating emerging technologies to help drive their businesses, as well as perceived skills and talent shortages.

FIGURE 24A

Technology, Media and Telecommunications — 2024

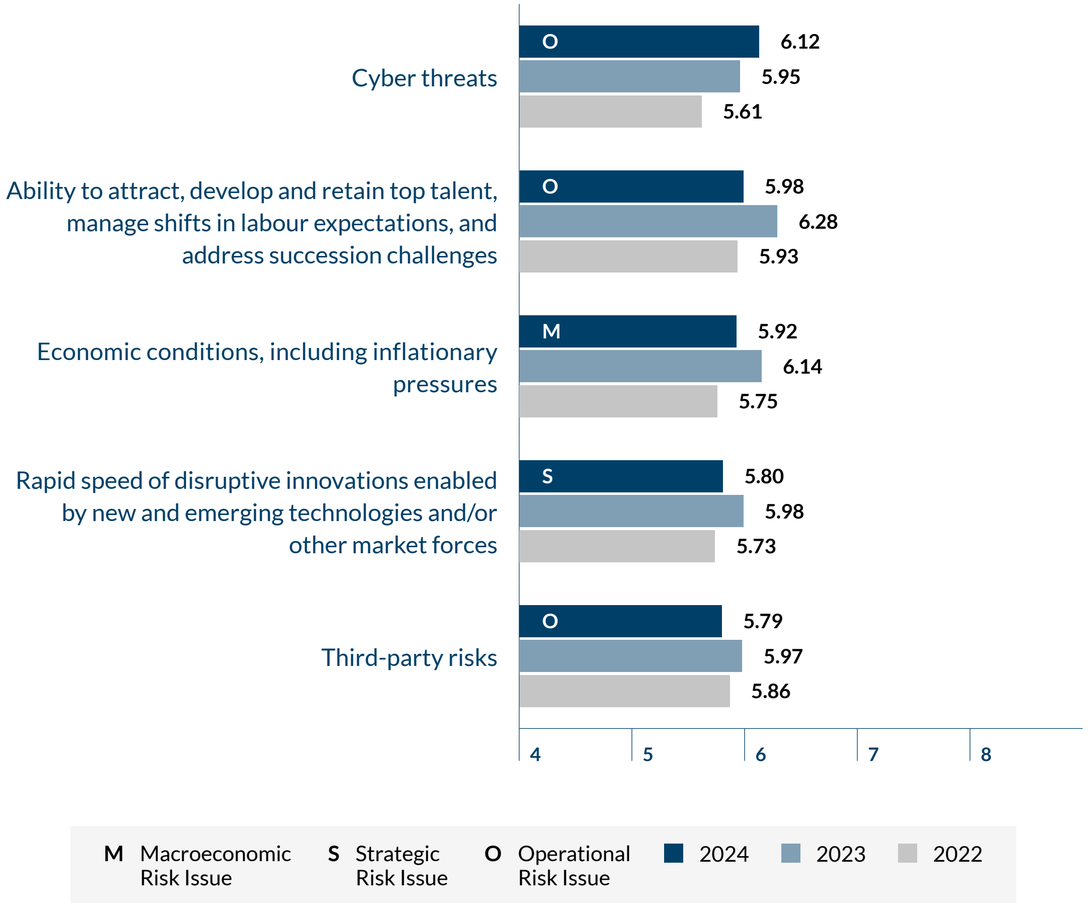
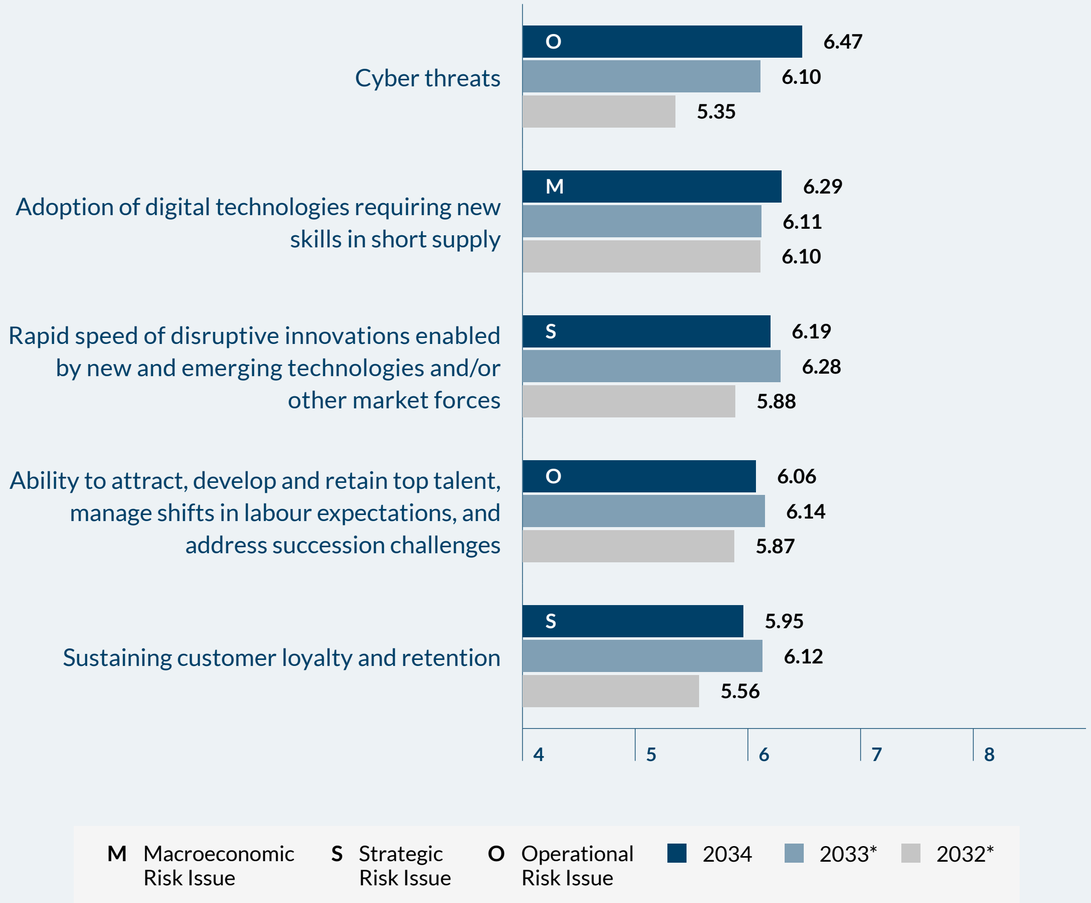


FIGURE 24B

Technology, Media and Telecommunications — 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.

Commentary — Technology, Media and Telecommunications Industry Group

BY GORDON TUCKER AND SCOT GLOVER
GLOBAL LEADERS, TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS INDUSTRY PRACTICE, PROTIVITI

Cyber threats have reemerged as the top risk concern for the Technology, Media and Telecommunications industry group, escalated by the continued expansion of attack vectors and geopolitical tensions. Labour constraints and economic conditions, including inflationary pressures, follow closely at No. 2 and No. 3 respectively, according to Protiviti's 2024 Top Risks Survey.

TMT executives were asked to identify the biggest threats they anticipate over the next 12 months and a decade ahead. Many of the risks cited correlate in many ways and can be categorised under two broad themes: foundational risks, which are essentially challenges that leaders must address to keep their business thriving, and risks that are essential for continued growth and expansion.

Cyber threats

Cyber threats have consistently ranked among the biggest risks confronting TMT executives. However, this year, global geopolitical tensions, including the Russian invasion of Ukraine and escalating trade tensions between the United States and China, have exacerbated the risk.

Insider threats are a significant concern, especially as companies navigate hybrid work models, putting more security responsibility on employees. The proliferation of artificial intelligence, cloud computing and the Internet of Things, which have significantly expanded the attack vectors, are also major factors.

Organisations must develop robust cybersecurity and insider threat protection and rapid response programs to protect their operations, which will allow for future growth.

Tackling the talent crisis

TMT organisations are also increasingly worried about their ability to attract, develop and retain top talent, manage shifts in labour expectations, and address succession challenges.

Since the pandemic, many companies have experienced unusually high attrition rates, although large multilocational organisations that have been able to accommodate employees seeking to relocate or transfer to different roles have been less impacted. High-level departures have also had devastating impacts on organisations. Replacing a C-suite executive or senior employee can be costly, although companies with deeper pockets, compared to startups and fledgling organisations, are able to absorb the impact better.

Overall, TMT companies, small and large, are struggling with succession planning. Many companies do not have documented succession plans and frequently fail to adequately communicate advancement pathways and development opportunities to valuable team members.

The talent gap extends also to the cyber workforce, where companies are desperate to train the next generation of cyber defenders. The weakening front line against cyberattacks may also explain why TMT executives are growing more nervous about cyber threats.

Inflationary pressures

Like the talent issue, pressure from inflation is hitting TMT companies in several different ways, depending on market share, pricing power and line of business, among other factors. Larger tech companies have been renegotiating favourable prices with their suppliers and many have been able to raise hardware prices and pass the higher costs to consumers. Those that do not have the same level of pricing power are contending with margin compression and aggressive cost cutting.

There are some signs that inflation may be cooling, but it remains at a level that has many executives up at night. TMT organisations, led by their CFOs, should lean on their data, predictive analytics and advanced technology tools to help them make better strategic decisions on ways to fight inflation.

Disruptive technologies

The impact of disruptive innovations and the ability to leverage new and emerging technologies to achieve growth is ranked fourth for 2024 by the TMT respondents. Closely related is a concern over the adoption of digital technologies requiring new skills in short supply, which is ranked the No. 6 top risk for 2024.

From artificial intelligence to wearable technology to nanotechnology to 5G, TMT companies have been the catalyst for many disruptive technologies, but they also have not been spared by disruptions associated with being on the cutting edge of technology.

In the telecommunications industry, for example, wireless carriers are competing not only with each other to advance 5G coverage and features but also with cable providers, who are looking to strengthen their position within the broadband market.[7]

Generative AI is another new technology that is upending the TMT industry. TMT finance leaders are already using generative AI for critical functions such as compliance and regulatory reporting. The technology is also fuelling fierce competition among companies whose chips enable ChatGPT. Clearly, the implications of adopting AI capabilities throughout the TMT industry and across society at large will continue to be a top risk for years to come.

Other top ten risks — and looking a decade ahead

Concern over third-party risks, ensuring privacy and compliance with growing identity protection expectations, and sustaining customer loyalty and retention are other 2024 top ten risk issues identified by TMT leaders.

Asked to project a decade ahead, TMT respondents cited cyber threats, adoption of digital technologies requiring new skills, and disruptive innovations as their top 3 risk issues.

[7] For more information, read Protiviti's white paper, *The 5G Effect — Lessons Learned from Real-World 5G Applications and the Roadmap Ahead*: www.protiviti.com/us-en/whitepaper/5g-effect.

FIGURE 25A

Healthcare — 2024

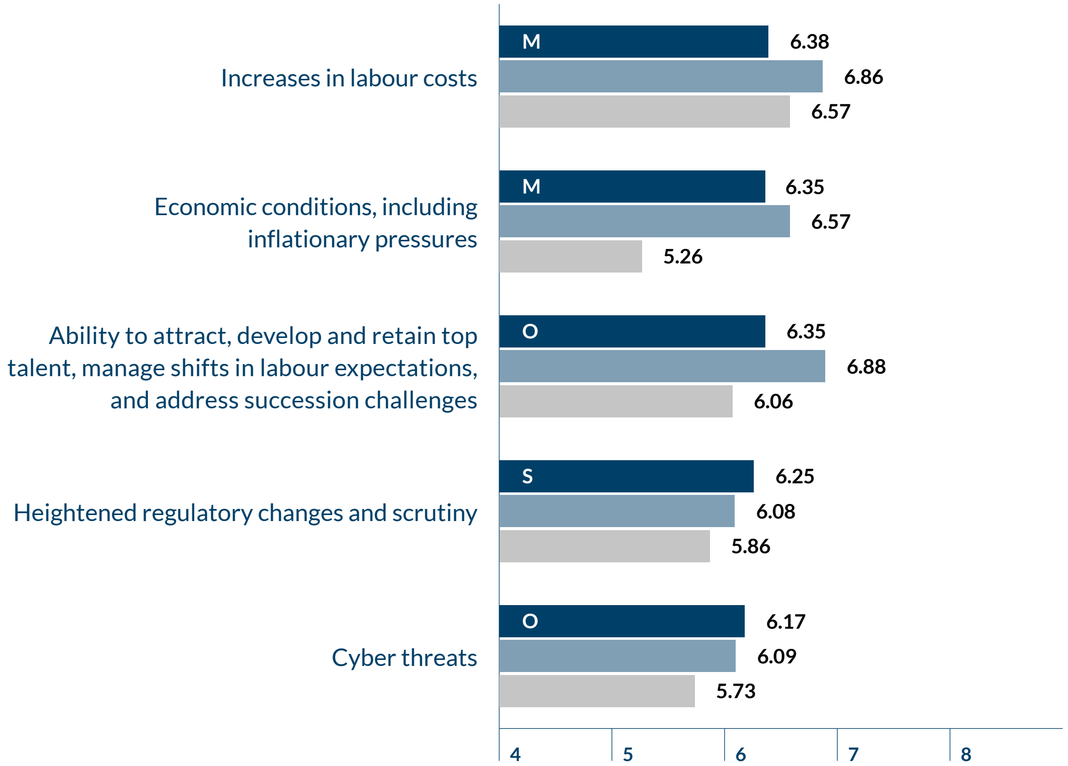
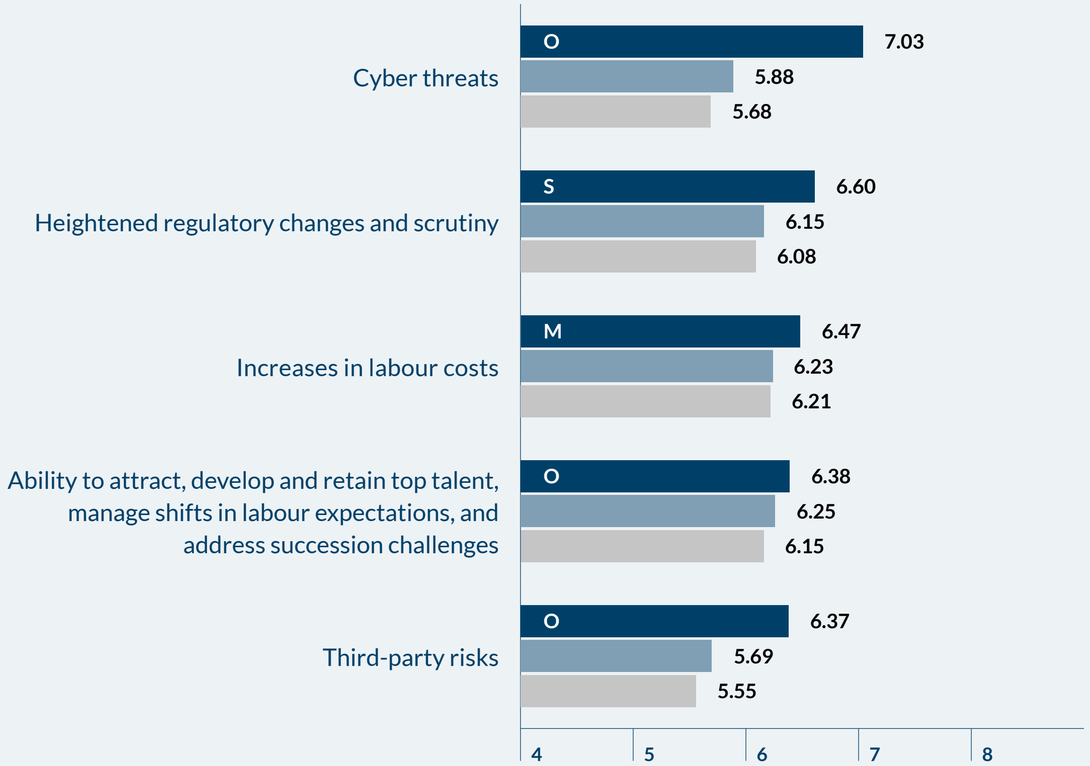


FIGURE 25B

Healthcare — 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.

Commentary — Healthcare Industry Group

BY RICHARD WILLIAMS
GLOBAL LEADER, HEALTHCARE INDUSTRY PRACTICE, PROTIVITI

Healthcare organisations continue to face familiar challenges as they look at the year ahead and a decade out. Rising labour costs and talent shortages, along with anticipated changes in the regulatory environment and continued economic and inflationary pressures, are forcing healthcare organisations and their respective boards to take a hard look at long-term challenges to their existing business models and plan for how they will transform their organisations to address these challenges now and for the long run.

Continued increases in labour costs are causing significant margin erosion

Across the healthcare industry, the number one risk for 2024 is the continuing increase in labour costs. The tightening of the healthcare labour market, exacerbated by the pandemic, has caused significant margin erosion, particularly on the provider side. Hospital labour expenses, which account for half of hospitals' total budget on average, increased by 20.8% between 2019 and 2022.[8] Expenses for contract labour, leveraged as a temporary solution since the onset of the pandemic, have increased 258% over the same timeframe.[9]

With healthcare workers leaving the industry at high rates due to factors such as burnout and ageing, it is imperative that the industry optimise and retain the labour that remains. The gap between staffing demand and supply has resulted in a 27% year-over-year increase in recruitment expenses. Additionally, healthcare saw an increase in organised labour activity in 2023, with contract demands for wage increases and better staffing conditions.[10] The macroeconomic factors driving increases in anticipated labour costs include inflation, shortages of both clinical and nonclinical workers, and continued fierce competition for healthcare workers with in-demand skills.

Risk associated with increased labour costs are predicted well into the future and remain in the top five concerns in 2034, dropping only two positions in rank. The World Health Organisation (WHO) Global Health Observatory model predicts that global demand for health workers will rise to 80 million by 2030 — twice the current supply — while the number of available health workers will reach only 65 million, resulting in a worldwide shortage of 15 million workers.[11] There is little relief in sight. Therefore, it will be essential to focus on worker productivity, establishing new ways of working by rethinking and redesigning jobs, and increasing the use of technology, particularly artificial intelligence (AI).

With healthcare workers leaving the industry at high rates due to factors such as burnout and ageing, it is imperative that the industry optimise and retain the labour that remains.

Economic conditions, including inflationary pressures, continue to erode margins

Globally, healthcare organisations continue to confront challenging economic conditions as rising healthcare costs,

[8] "New AHA Report Finds Financial Challenges Mount for Hospitals & Health Systems Putting Access to Care at Risk," American Hospital Association: www.aha.org. www.aha.org/press-releases/2023-04-20-new-aha-report-finds-financial-challenges-mount-hospitals-health-systems-putting-access-care-risk.
[9] Ibid.
[10] "Healthcare labour union activity gains steam: The consequences for hospitals and health systems," Healthcare Financial Management Association: www.hfma.org/finance-and-business-strategy/healthcare-business-trends/healthcare-labour-union-activity-gains-steam-the-consequences-for-hospitals-and-health-systems/.
[11] "Global Health Workforce Labour Market Projections for 2030," Liu, Jenny X., Yevgeniy Goryakin, Akiko Maeda, Tim Bruckner, and Richard Scheffler, Human Resources for Health 15 (1), 2017: https://doi.org/10.1186/s12960-017-0187-2.

inflation, labour shortages and COVID-endemic recovery contribute to below-average operating margins, although there is improvement from pandemic lows.

Healthcare provider margins are improving at a much slower rate compared to the payer side. The healthcare provider services market grew at a compound annual growth rate (CAGR) of 6.3% between 2022 and 2023 (with an anticipated CAGR of 5.3% in 2027),[12] while the healthcare payer services market has an anticipated CAGR of 7.71% by 2027.[13] Median margin data indicate that half of U.S. hospital and health systems continue to operate at a financial loss, with many just covering their costs in 2023.[14] This is understandable as hospitals' total costs, including labour costs, increased 17.5% during the pandemic.

Outside of reimbursement rate hikes and growth in market share, healthcare organisations must look to cost-cutting measures and improvements in productivity and performance to improve margins. Transformational change will be required of organisations to maintain or return to positive operating margins as the global population continues to grow and age and value-based care models continue to be adopted and evolve. Across the board, there is potential for increased costs driven by volume. If organisations cannot balance the costs and healthcare spend of consumers, the organisations risk operating on narrow margins.

Looking toward 2034, care delivery will continue to become more digital. Population health efforts will guide patients to the most appropriate care setting more efficiently and with greater care coordination. Successfully combining digital capabilities with population health efforts will provide for a higher quality of care at a much greater value, and the efficiencies gained should yield a positive operating margin.

Tools that support clinical decision-making, predictive analytics and remote/hybrid work are expected to enable a shift from people-driven to technology-supported models of care.

Ability to attract and retain talent and address succession challenges remains a critical issue

The ability to attract and retain top talent in a continually tightening labour market remains one of the top five risks for healthcare organisations for the third consecutive year. The crisis in healthcare human resources has been described as one of the most pressing global health issues of our time, as the WHO estimates a global shortage of 15 million healthcare professionals by 2030.[15]

Almost one in three healthcare workers are considering leaving the industry due to burnout, job dissatisfaction and heavy demands for productivity and efficiency.[16] Throughout the industry, the largest staffing concern and resulting pain point over the last few years has been clinical staff retention.[17] This troubling trend impacts not just the bottom line; it also can diminish the accessibility and quality of patient care. Innovative strategies are needed to meet current and future staffing demand through different approaches to attract, hire, train, retain, support and transform the workforce.

[12] "Healthcare Services Global Market Report 2022": www.reportlinker.com/p06229152/Healthcare-Services-Global-Market-Report.html?utm_source=GNW.
[13] "Global Healthcare Payer Services Industry Research Report, Competitive Landscape, Market Size, Regional Status and Prospect," Absolute Reports, September 13, 2022: www.absolutereports.com/global-healthcare-payer-services-industry-research-report-competitive-landscape-market-21703171.
[14] "Costs of Caring," American Hospital Association, 2023, April 2023: www.aha.org/costsofcaring.
[15] "Health Workforce," World Health Organisation, August 7, 2019: www.who.int/health-topics/health-workforce#tab=tab_1.
[16] "The Association of Work Overload with Burnout and Intent to Leave the Job across the Healthcare Workforce during COVID-19," Rotenstein, Lisa S., Roger Brown, Christine Sinsky, and Mark Linzer, 2023: Journal of General Internal Medicine 38 (8): https://doi.org/10.1007/s11606-023-08153-z.
[17] "2023 NSI National Health Care Retention & RN Staffing Report," NSI Nursing Solutions, Inc. 2023: www.nsinursingsolutions.com/Documents/Library/NSI_National_Health_Care_Retention_Report.pdf.

Healthcare organisations view this risk as a long-term concern, ranking it the fourth highest anticipated risk for 2034. Transforming the workforce through a combination of job redesign, improved automation and reskilling/upskilling workers will create new career pathways, critical to engaging and retaining workers. AI and emerging digital technologies will continue to transform how healthcare is delivered. Tools that support clinical decision-making, predictive analytics and remote/hybrid work are expected to enable a shift from people-driven to technology-supported models of care.

Heightened regulatory changes and scrutiny are continuing concerns

Maintaining and managing compliance with continual regulatory changes and heightened regulatory scrutiny ranks as the fourth-highest challenge for healthcare organisations in 2024. The U.S. federal budget contains greater funding than in prior years for enforcement, especially related to healthcare fraud and investigative efforts. Priority areas include, but are not limited to:

- Price and drug cost transparency
- Access to quality care
- Cybersecurity
- Privacy (with potentially a new HIPAA regulation)
- Medicare Advantage changes
- Clinical research
- Mental health

Changes in the regulatory environment, including requirements around the use of technology, will be a constant for the healthcare industry well into 2034, heightening focus on data security and privacy.

Cross-agency collaboration will likely continue to rise, especially as data analytics become more sophisticated. In 2023, the U.S. Department of Justice, together with federal and state law enforcement partners, brought charges against 78 defendants for their alleged participation in fraud and opioid abuse schemes, which included over $2.5 billion in alleged fraud.[18]

In November 2023, the U.S. Department of Health and Human Services Office of Inspector General (HHS-OIG) published new General Compliance Program Guidance for the healthcare industry, addressing topics such as federal fraud and abuse laws, compliance program basics and operating effective compliance programs. Additional segment-specific guidance is promised, addressing topics including compliance risk areas, compliance program best practices, and common pitfalls.[19] This is another indicator that the government is becoming more serious about healthcare organisations having effective compliance programs.

Changes in the regulatory environment, including requirements around the use of technology, will be a constant for the healthcare industry well into 2034, heightening focus on data security and privacy. Regulations and enforcement associated with access to care and patient protections also will remain at the forefront, including protections to facilitate health equity. Data analytics, automation and AI will continue to mature and play a key role in fraud and abuse crackdowns across the industry.

[18] "National Enforcement Action Results in 78 Individuals Charged for $2.5B in Health Care Fraud," U.S. Department of Justice, June 28, 2023: www.justice.gov/opa/pr/national-enforcement-action-results-78-individuals-charged-25b-health-care-fraud.
[19] "Modernisation of Compliance Program Guidance Documents," U.S. Office of Inspector General, November 2023: https://oig.hhs.gov/documents/compliance-guidance/1114/GCPG-ICPG-Federal-Register-Notice.pdf.

Cybersecurity, data privacy and identity protection are a key focus

Cybersecurity remains a top concern for healthcare leaders and their respective boards. Ransomware incidents are particularly perilous, as they can disrupt critical healthcare systems, putting patient safety and organisational revenue, compliance and reputation at risk. Because they have more to lose, healthcare providers and payers are prime targets.

The inherent complexity of data environments within healthcare, with numerous entry and exit points, further exacerbates the challenge of protecting patients and their data. Additionally, the altruistic nature of many healthcare professionals makes them especially susceptible to social engineering tactics. Outdated technology systems prevalent in healthcare further compound the problem by introducing technical vulnerabilities, particularly if they haven't kept up with regular security updates.

Other emerging technologies, including the rise of AI, the potential ubiquity of quantum computing, the expansion of the Internet of Things (IoT), and the unceasing wave of digitisation further add to the complexity. The continuing need to foster better interoperability in the healthcare ecosystem only intensifies the need for robust cybersecurity measures. Healthcare organisations must diligently plan for and invest in an enduring cybersecurity enhancement program.

Evolving regulatory requirements and increased risks of noncompliance will continue to increase the criticality of a comprehensive third-party risk management strategy.

For 2034, cyber threats are expected to be the number one risk for healthcare organisations, as they continue to be challenged with recruiting and retaining a specialised workforce capable of staying ahead of cyber adversaries. This will require deep technical data security skills and the ability to understand the complicated environments in which healthcare payers and providers operate.

Cybersecurity must be an ongoing journey. Its programs require unwavering investment, meticulous staffing, cutting-edge tooling, continuous enhancement, rigorous assessment, relentless testing and comprehensive training across the vast tapestry of a healthcare organisation's internal practices, partnerships and vendor relationships.

While not in the top five risks for 2024, reliance on third-party vendors continues to be an emerging long-term issue for healthcare organisations, ranking as the fifth-highest risk for 2034. As healthcare organisations struggle to keep up with emerging technologies and margin pressures, failure to manage vendor risks can leave them exposed to regulatory action, business outages, financial losses, litigation and reputational damage, and can impair the organisation's ability to gain new or service existing customers. Evolving regulatory requirements and increased risk of noncompliance will continue to drive the need for a comprehensive third-party risk management strategy.

FIGURE 26A

Energy and Utilities — 2024

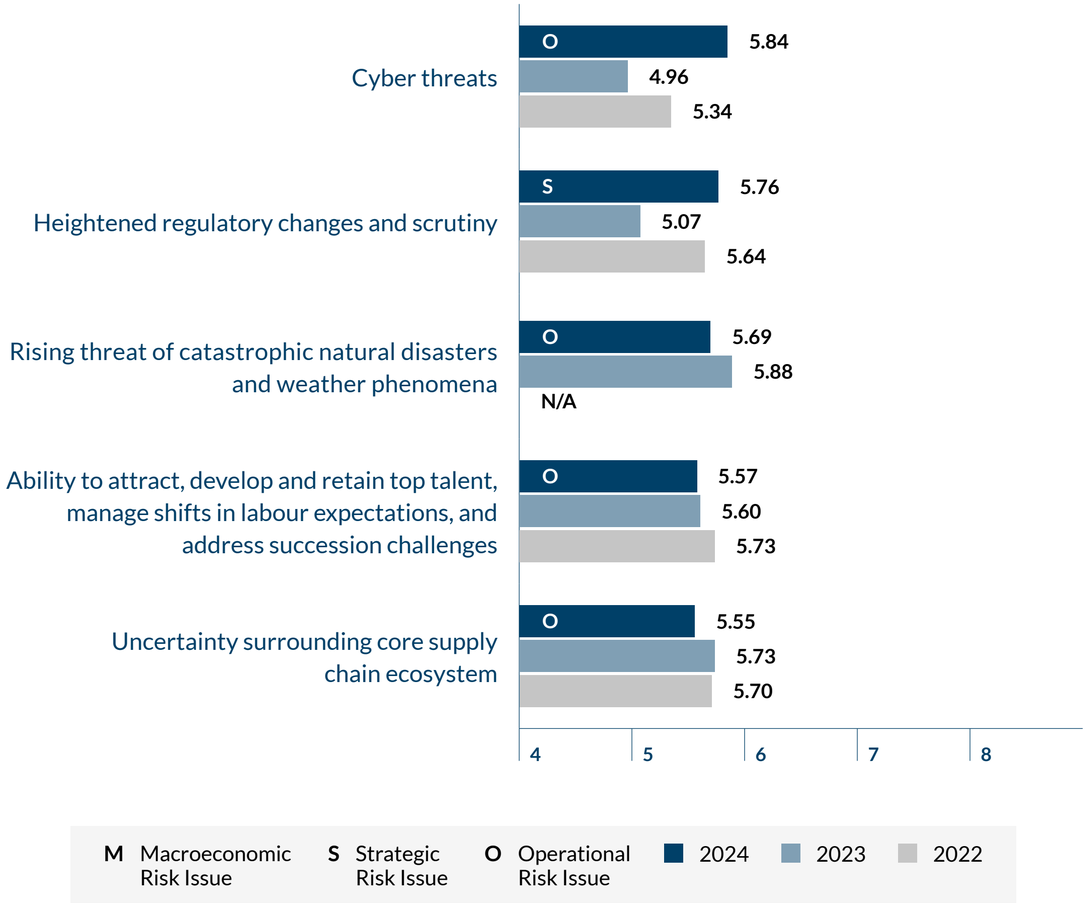
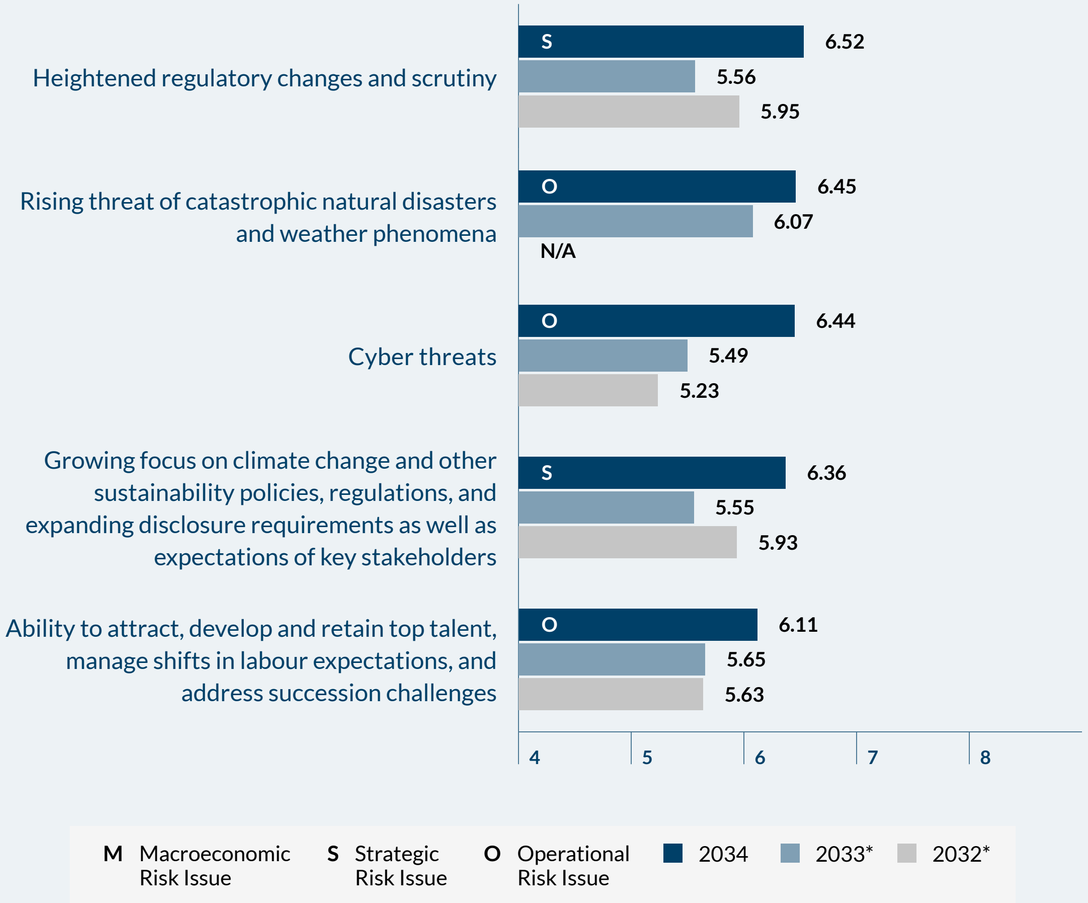


FIGURE 26B

Energy and Utilities — 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.

Commentary — Energy and Utilities Industry Group

BY TYLER CHASE
GLOBAL LEADER, ENERGY AND UTILITIES INDUSTRY PRACTICE, PROTIVITI

Resistance to change has long been a hallmark of the energy and utilities industry. But forward-thinking leaders are realising that the only status quo that will allow their businesses to evolve operationally, digitally and culturally to meet new demands and expectations, drive innovation, and help shape the energy industry of the future is one of continuous change and strategic risk-taking.

Energy and utilities companies have been under increasing pressure for years to modernise their operations and evolve to new business models that focus on sustainability. But transformation has been a slow and challenging process for many of these organisations, largely because of substantial capital investments in the field with operations that serve the needs of the business for many years. A proof point is the presence among the top 10 risks for this sector, year after year, of the operational risk "Resistance to change in our culture may restrict our organisation from making necessary adjustments to the business model and core operations on a timely basis."

However, in our latest survey, things are markedly different. In 2023, resistance to change ranked sixth, but on the 2024 list, it has tumbled to 12th. Looking further out into the future, we see an even more dramatic drop in the level of concern for this risk. Industry leaders ranked it second last year on their list of top risks for the next decade — but this year, it has plummeted to 22. That this risk is no longer viewed as a key concern, especially over the longer term, suggests that many energy and utilities executives now see change as the "new normal" for their companies and industry.

The recent pandemic's disruption is certainly one factor for this shift in attitude toward change — particularly, the need to adapt to it and to drive it as a way to increase agility and resilience. But there is also recognition in this industry that the shift toward more renewable and sustainable activities will continue and likely accelerate, and companies must respond effectively to that. Some energy and utilities businesses have already created a roadmap for how they want and need to make an energy transition over time, and thus have more confidence about pursuing change.

Rapid advancements in technology and a need to be more agile are also breaking down the resistance to change within energy and utilities companies. More to the point, there is greater acceptance in their organisational cultures that this type of change is inevitable — and necessary. Many companies in the industry are well along with their digital transformation efforts and are looking to evolve further to take advantage of the latest trends, like AI. And as they, and their competitors, start to realise bottom-line benefits from their investments, resistance to change as an operational risk will continue to fade.

Cyber threats and increased regulatory pressure top the risk leaderboard for 2024

In our previous Top Risks Survey, we found that operational issues were a priority focus for energy and utilities leaders in 2023. The same is true for 2024, although the top-five lineup now includes a strategic risk in the No. 2 spot: heightened regulatory changes and scrutiny. That this risk has catapulted into the top five from 16th place in 2023 indicates that industry leaders are likely wondering what the outcome of this election cycle could mean for the future regulatory landscape.

Mandates related to ESG issues — particularly, greenhouse gas emissions reporting — are also top of mind for leaders in the industry. They also see this as an ongoing challenge for their organisations: They rank this risk fourth among the top concerns for the industry in 2034, pulling it up from eighth place on the 10-year outlook list last year.

One operational risk that has skyrocketed into the top five for 2024 is cyber threats, up from 17th place last year. This is an acknowledgement by energy and utilities executives that their critical infrastructure businesses are, and will remain, a focus for adversaries.

Ransomware is an ongoing concern for this industry, as are supply chain attacks. And while businesses in this industry have transformed digitally to a large degree, particularly in their back-office operations like finance and accounting, many still rely heavily on legacy technology, like SCADA systems, for industrial operations, which can be vulnerable to attack. The adoption of new technology to be more connected to the field also creates new security risks for energy and utilities companies.

Supply chain uncertainty has lessened — but remains a key concern

Rounding out the top five risks for 2024 is "uncertainty surrounding our organisation's core supply chain." This risk dropped from second place on last year's list, which suggests that pandemic-driven supply chain disruption in areas such as production and delivery has eased. Many companies in the energy and utilities industry have also made a concerted effort in recent years to modernise their supply chain and make it more resilient. That includes developing formal supply chain capabilities and investing in new technologies to increase visibility and predictability.

What hasn't changed for the industry, though, is how reliant energy companies are on their supply chains in general. We have reported this in previous Top Risks Survey reports, but it is worth underscoring once again that supply chain risk is both significant and persistent for the energy industry because its value chain is highly service-, feedstock-, parts- and equipment-oriented.

Another factor contributing to uncertainty about supply chain viability may stem from the fact that many companies in the energy and utilities industry are embracing new business models and innovating new products and services. Thus, they may be facing the need to alter the makeup of their supply chain ecosystem to support those initiatives and work with new and untested partners.

Worries about changing workplace dynamics and weather-related risks have also eased

In our previous Top Risks Survey, it was clear that evolving workforce dynamics were weighing heavily on the minds of many executives in the energy and utilities industry. But a year later, it appears those worries have largely subsided.

Challenges in sustaining culture due to change in the overall work environment, like the shift to hybrid work, is an operational risk that has diminished, dropping from fourth place on the 2023 list to 14th for 2024. Also, the risk of managing demands on or expectations of the workforce to work remotely or as part of a hybrid work environment fell from fifth place last year to 25th in this year's survey.

However, it is worth noting that the leaders of energy and utilities businesses are still concerned about the risk pertaining to their organisation's ability to attract, develop and retain top talent, manage shifts in labour expectations, and address succession challenges. The ranking of this risk changed only slightly from last year's survey, moving from third to fourth place. This indicates that many energy and utilities companies are still struggling to recruit an ample supply of talent to replace retiring workers and take on new jobs that require specialised skills and digital savvy. Another ongoing challenge is attracting younger professionals, many of whom prioritise working for sustainable companies, to take a job in an industry that they associate with unfavourable environmental impacts.

Energy and utilities executives are also somewhat less concerned than they were a year ago about their companies facing operational challenges due to extreme weather threats. The No. 1 risk cited by these leaders last year was the rising threat associated with catastrophic natural disasters and weather phenomena creating significant operational challenges that threaten a company's assets, employees, and ability to deliver products and services to customers. This year it ranks third, after cyber threats and regulatory changes.

This risk's slight slide within the top-five ranking may be another indicator that energy and utilities companies are coming to grips with the idea of change — and disruption — as their new status quo. Extreme weather events are, unfortunately, the new normal. In 2023, we saw historic heat, wildfires and storms, all of which had impacts on critical energy infrastructure in one way or another. And the reality is, no matter how much an oil and gas company or an electric utility does to increase its resilience and protect its infrastructure, no measure is 100% foolproof against the unpredictable forces of nature.

Looking ahead: The top risks for 2034 at a glance

The energy and utilities executives who responded to our latest Top Risks Survey anticipate that their businesses will be focused on managing a mix of operational and strategic risks in 2034.

The two strategic risks are related to regulatory pressures: heightened focus on regulatory changes and scrutiny and growing focus on climate change and other sustainability policies, regulations and expanding disclosure requirements as well as expectations of key stakeholders. These findings signal that industry leaders expect their industry, which is already highly regulated, is poised to become even more so as the focus on climate change, sustainability and other issues continues to intensify.

Cyber threats, an operational risk, ranks third among the top five risks for 2034, moving up from 11th on last year's list looking out 10 years. Leaders in the energy and utilities industry clearly understand that their businesses will likely remain a favoured target for cyber attackers, including nation-state actors. However, that the cyber threats risk does not rank first, as it does on the 2024 list, may be a sign that these executives are hopeful they will have better cyber defences in place by 2034 — including intelligent, AI-powered solutions that can keep pace with rapidly evolving threats.

The rising threat of catastrophic natural disasters and weather phenomena is another key concern for 2034, but it has dropped to second place after ranking first on last year's list. Industry leaders also foresee continued challenges in attracting talent; this operational risk moves up to the fifth spot from sixth place in the previous year's top risks ranking.

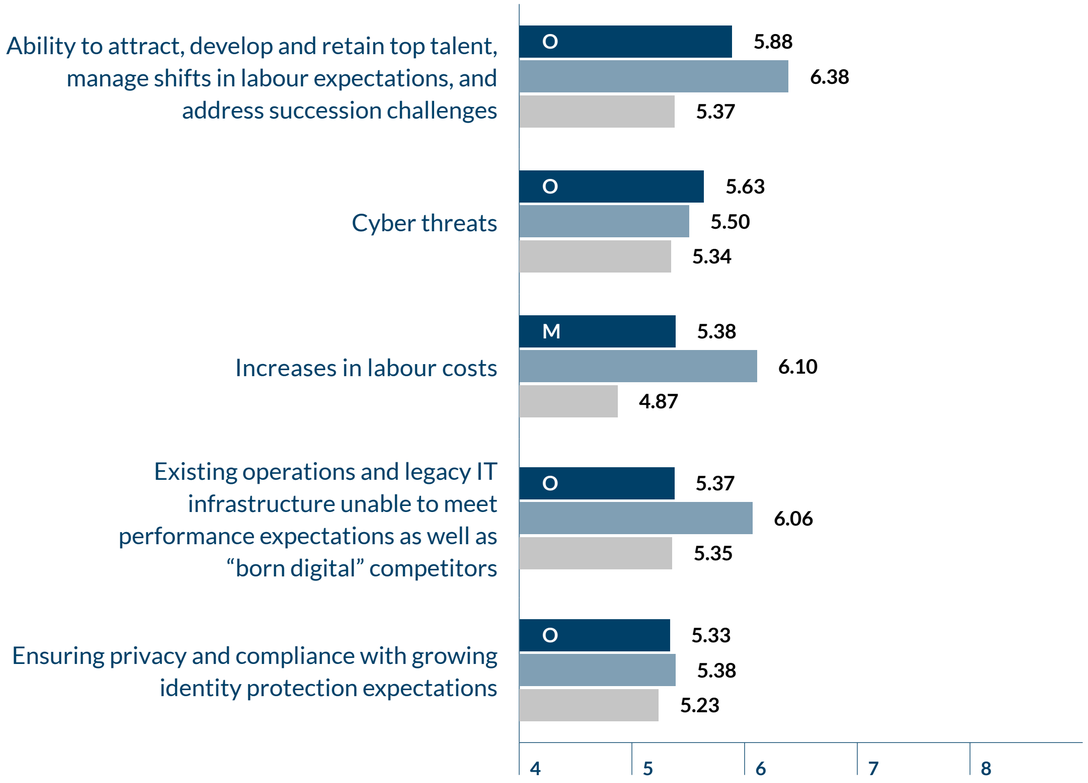
Notably, we see risks related to the adoption of digital technologies and the ability to use data analytics for competitive advantage falling out of the top five list for energy and utilities companies in 2034. In fact, the latter risk ranks 14th, dropping from fourth place. Concerns about the rapid speed of disruptive innovation, which was fifth last year, is still in the top 10 — ranking seventh.

These findings suggest executives with energy and utilities companies may be confident that their organisations will have undergone significant transformation by 2034. But given how quickly things change with technology and how much the energy industry itself is changing, they may also worry that their businesses will still be at risk of falling behind and failing to compete effectively.

Another sign of that emerging concern is the presence of the following strategic risk in the No. 8 spot, up from 25th on last year's list: Substitute products and services may arise from competitors that enhance the customer experience and affect the viability of our current business model and planned strategic initiatives. This isn't surprising given the growing investments in clean energy innovation and a belief that newer advancements will need to be made in order to provide the amount of clean energy needed. Maintaining an openness to change and having the agility to adopt new technologies over the next decade may be exactly what energy and utilities businesses need to do to keep that potential risk at bay — or, at least, minimise its impacts.

FIGURE 27A

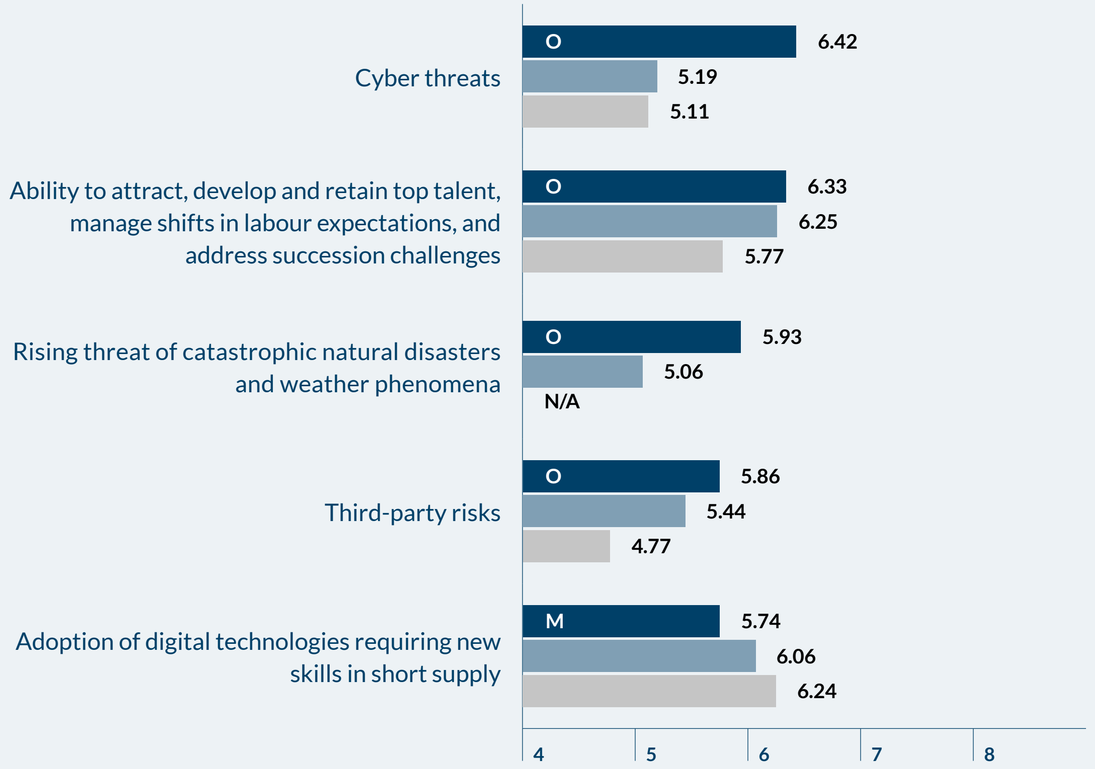
Government — 2024



M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue 2024 2023 2022

FIGURE 27B

Government — 2034



M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue 2034 2033* 2032*

* 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.

Commentary — Government Services Industry Group

BY CHARLES DONG
GLOBAL LEADER, PUBLIC SECTOR INDUSTRY PRACTICE, PROTIVITI

With a few notable exceptions, the global risk landscape for government services organisations (specifically, agencies and departments within the government sector) in 2024 and 2034 looks similar to our survey results from the past two years. However, the fact that issues related to talent, cyber threats and legacy IT infrastructure remain ongoing — and in many cases intensifying — concerns for government services leaders may reflect the need for wholesale changes in how these risks are addressed and mitigated.

This is the case because the nature, magnitude and causes of these challenges remain anything but steady. The methods that bad actors (including but not limited to nation-states) deploy to breach cyber defences continue to evolve at an accelerating pace at the same time that attack vectors are expanding throughout government agencies due to digital accessibility and other factors. This explains why cyber threats are rated as a higher concern for 2024 than they were in last year's survey for 2023 — and also why they expect cyber threats to become significantly more problematic by 2034.

The ability of government organisations to attract, develop and retain top talent, manage shifts in labour expectations, and address succession challenges faces additional headwinds as labour costs remain high and as an outsized portion of the public-sector workforce nears retirement age. The scope, cost and time required to replace legacy IT systems are also increasing. Outdated technology systems limit government services organisations' ability to meet performance expectations and to respond with speed and efficacy to unexpected crises.

As leaders of government services organisations focus their attention on the most pressing and prevalent risks in 2024, they should consider new mindsets and approaches for managing talent, mitigating cyber threats and updating legacy IT infrastructure.

Overview of top risk issues in 2024

While most of the top risk issues for the government services sector in 2024 relate to talent, cybersecurity and legacy IT environments, organisational culture and resilience also represent urgent concerns, as does the ability to respond to unexpected crises with resilience and agility. Government services leaders express reservations regarding the degree to which their organisational cultures encourage the timely identification and escalation of emerging risk issues. Whether the organisation can respond effectively and in an agile manner to unexpected crises marks another top concern.

As leaders of government services organisations focus their attention on the most pressing and prevalent risks in 2024, they should consider new mindsets and approaches for managing talent, mitigating cyber threats and updating legacy IT infrastructure. Doing so requires a solid grasp of the multifaceted nature of these issues.

- **Talent management:** Attracting, recruiting and retaining skilled workers are ongoing — and borderline endemic — challenges within government services. These areas also represent a long-term problem: Survey respondents project talent-related risks as the second most significant concern in 2034, just behind cyber threats (see below). The historic allure of government service (e.g., situations such as the Cold War and Space Race, which provided strong, non-financial motivation) does not appear to be motivating younger workers to pursue government employment in the way people did in the latter half of the 20th century. Now, more "baby boom" engineers who leapt at the opportunity to work

for space programs in the 1960s, 1970s and 1980s are retiring, and Gen X workers may not be far behind. From 2020 to 2022, an average of more than 100,000 U.S. federal workers retired each year. That's 36% higher compared to the period from 2000 to 2002, when approximately 76,000 federal workers retired annually.[20] Retirement-age federal employees now outnumber younger employees by two to one in the United States, where there were more full-time permanent federal employees in the 50—54 age bracket than any other age group in 2022.[21] Furthermore, across the globe, subsequent generations are far more likely to choose the allure and higher pay of jobs in industries such as technology and financial services over government roles. Of note, for 2024, other talent management-related concerns include increasing labour costs (the third highest-ranked risk issue) and the impact of social issues and DEI priorities on organisations' ability to attract and retain workers (a top 10 risk issue).

- **Cybersecurity:** As is the case with talent management, cyber threats are an area of significant concern for government agencies. To illustrate, in the United States, over the past dozen years or so the U.S. Government Accountability Office (GAO) has publicly issued more than 700 recommendations related to securing federal systems and information. "Until these are fully implemented," a January 2023 GAO report states, "federal agencies will be more limited in their ability to protect private and sensitive data entrusted to them."[22] Not surprisingly, ensuring privacy and compliance with growing identity protection expectations also ranks as a top 2024 risk issue among government services respondents. The same holds true for third-party risks (ranked in the top 10 for 2024), many of which relate directly to data privacy and security issues.

  As government services leaders address cybersecurity, they should keep in mind that attack surfaces are expanding due to digital transformation progress (including the widespread shift to online services) and the increasing adoption of Internet of Things (IoT)-connected networks and applications. IoT sensors generate more data and provide bad actors, who continually develop new modes of attack, with new opportunities to breach organisational cyber defences. Smaller government organisations, including those at the regional, province/state, and local levels, are especially vulnerable to cyber threats. Smaller agencies and departments generally have more limited cybersecurity budgets and less access to the knowledge and skills required to create and continually adapt their cybersecurity capabilities to new types of threats and attack modes. At the same time, because these organisations are perceived to be easier targets to breach, bad actors increasingly are targeting them to disrupt operations and interfere with elections through phishing, denial of service and ransomware attacks.

As government services leaders address cybersecurity, they should keep in mind that attack surfaces are expanding due to digital transformation progress (including the widespread shift to online services) and the increasing adoption of IoT-connected networks and applications.

- **Legacy IT:** Government services organisations face scale, time, money and resource challenges when it comes to addressing ageing IT infrastructures through technology modernisation. Mainframe systems designed in the 1970s and 1980s still underpin operations in many government offices. These infrastructures have been held together with numerous makeshift, ad hoc solutions by systems administrators who have already retired or will do so soon. In addition, given their age and design, many legacy systems have undergone extensive customisation. In many cases, this means that upgrades are off the table, and that new, modern systems must be

[20] www.opm.gov/retirement-center/retirement-statistics/.
[21] https://usafacts.org/articles/how-old-is-the-federal-workforce/.
[22] www.gao.gov/products/gao-23-106428.

implemented from scratch. While time-consuming and expensive, such implementations are crucial to perform because outdated systems can limit organisational resilience and agility (another top 10 risk concern for 2024) as well as the ability to recruit talented technology professionals who would rather work with advanced tools and technologies than perform troubleshooting and maintenance on antiquated systems. Additionally, more large ERP vendors are establishing definitive timelines for moving customers away from on-premises solutions to cloud environments, further underscoring the urgency to update legacy systems.

It is worth noting that ongoing political polarisation and legislative gridlock frequently hinder the ability of government services organisations to respond to many of these risk issues. Budgeting brinkmanship at all levels of government injects additional uncertainty into planning and forecasting activities.

Intensifying geopolitical concerns reflect the wars in Ukraine and the Middle East as well as rising tensions between China and Taiwan, among other flashpoints.

Overview of top risk issues in 2034

When government services leaders share their 10-year outlook, cybersecurity and talent management risk ratings are considerably higher, and they are joined by major concerns related to natural disasters and regulatory requirements focused on climate change and sustainability.

In last year's survey, the rising threat of catastrophic natural disasters and weather phenomena barely rated as a top 25 risk concern. For 2024, this risk issue figures as a top 15 concern. By 2034, government services leaders rank the threat of natural disasters in their top five (specifically, third), with sustainability policies, regulations and disclosure requirements not far behind.

Catastrophic natural disasters are not the only concern that government services survey respondents expect to become riskier during the next decade. Compared with last year's survey results related to the long-term risk outlook, this year's respondents gave notably higher risk ratings to many of their longer-term concerns — including cyber threats, third-party risks, and geopolitical shifts, regional conflicts and instability in government regimes or the expansion of global terrorism.

Of note, similar to the roadblocks government agencies face with their 2024 top risks, political polarisation and gridlock may inhibit their ability to respond to these issues effectively.

Heightened geopolitical concerns reflect intensifying conflicts around the world. The survey results indicate an expectation among government leaders that the current period of geopolitical conflict will sustain over the coming decade. Government services leaders also view cyber threats and talent-related risks as long-term challenges. Heightened regulatory changes and scrutiny along with organisational culture concerns (centred on the timely identification and escalation of emerging risk issues) round out the list of highest-rated 2034 risk issues.

Analysis across geographic regions

As in prior years, we obtained responses from enough organisations across the globe to explore results from eight distinct regions. We analyse responses across these eight regions to determine whether respondents across different geographic locations rank-order risks differently. Similar to our analysis summarised earlier in this report, we analyse responses about overall impressions of the magnitude and severity of risks across the eight regions.

The scores in Figure 28 reflect responses to the question about the overall impression of the magnitude and severity of risks using a 10-point scale where 1 = "Extremely Low" and 10 = "Extremely High."

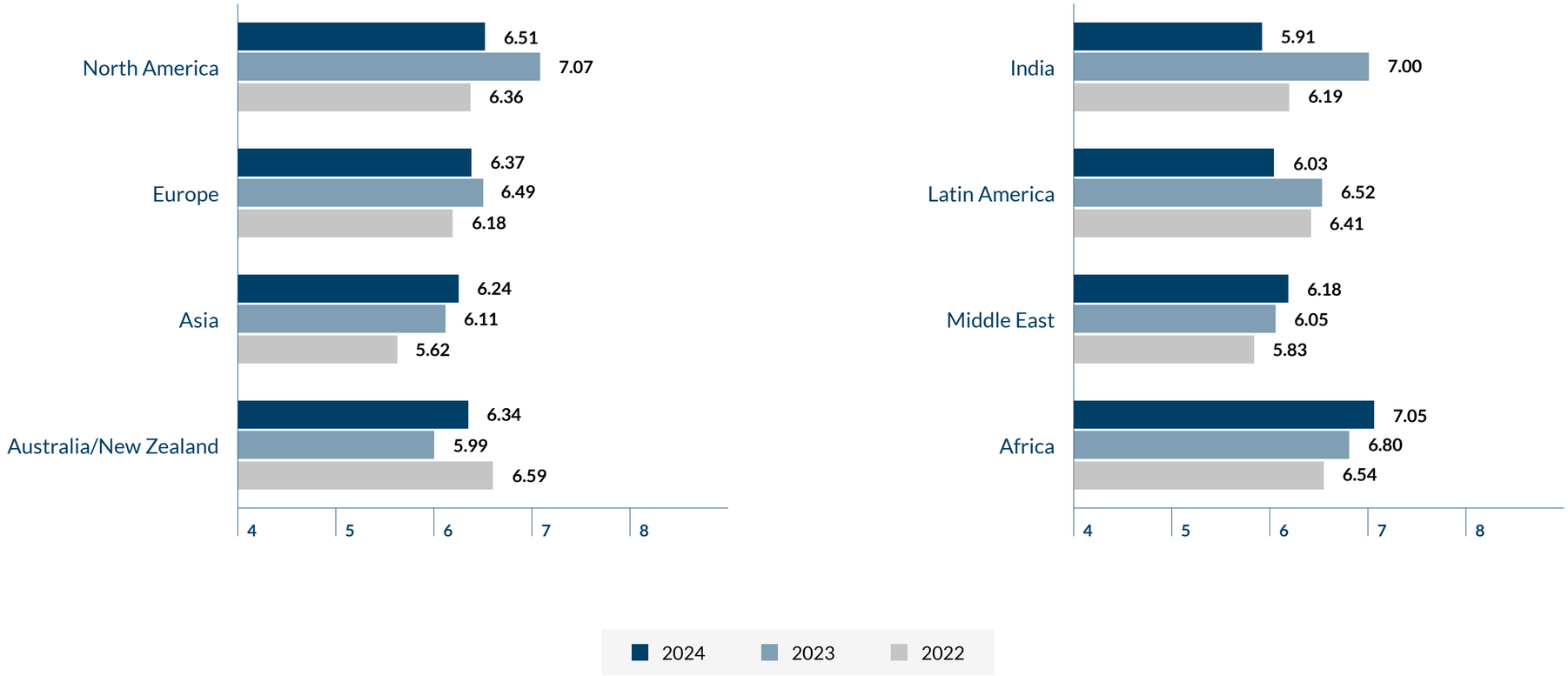
Geographic region	Number of respondents
North America	488
Asia	128
Australia/New Zealand	88
India	78
Europe (includes U.K.)	187
Latin America	99
Middle East	56
Africa	19
Total number of respondents	**1,143**

"Four of the eight regions we explore reveal heightened overall risk concerns for 2024 relative to the prior year. As well, all but India report an overall level of concern that maps to our designation as a Significant Impact risk (i.e., greater than 6.0)."

BRUCE BRANSON
ALUMNI DISTINGUISHED PROFESSOR OF ACCOUNTING
POOLE COLLEGE OF MANAGEMENT
NC STATE UNIVERSITY

FIGURE 28

Overall, what is your impression of the magnitude and severity of risks your organisation will be facing with respect to achieving your performance goals over the next 12 months?



Organisations from seven of the eight geographic regions agree that the overall magnitude and severity of risks are of a "Significant Impact" level for 2024. Only organisations in India rate the severity and magnitude of 2024 risks below 6.0. Four of the eight regions rate the magnitude and severity of risks as more severe than 2023, while the remaining four perceive a reduction in the overall magnitude and severity of risks moving from 2023 to 2024. North American organisations as well as those from Africa exhibit the largest level of risk concern for 2024, with both regions rating the overall magnitude and severity of risks at 6.50 or higher.

2024 risk concerns

Figures 29-36 highlight the top five risks from each of the eight geographic regions we examine and include the risk scores for 2024 and, separately, for 2034, as well as, where available, scores for those risks reported in our 2023 and 2022 reports. There are noticeable differences in views about risks around the globe, which is especially important for multinational organisations to consider. Fifteen of the 36 risks appear among the eight geographic regions as top five risks. Operational risks dominate, with at least three of the top five risk issues in each region (with the exception of Asia (two)) being operational in nature.

Consistent with our full sample results, the risks associated with succession and talent acquisition and retention and economic conditions are top of mind for many regions. All eight regions included succession risks and talent acquisition and retention in their top five. Six of the eight regions similarly include the risk associated with economic conditions among their top five risk concerns for 2024. Only two strategic risks are included among the top five for any of the regions in 2024: risks associated with regulatory change and enhanced scrutiny, and social media developments and platform technology innovations.

2034 risk issues

Looking further out into 2034, strategic risks become more heightened for all regions. Fourteen different risks appear in the top five across the eight regions, with six of these being strategic risks, four operational risks and four macroeconomic risks. The two most commonly cited top five risks, each appearing in seven of the eight regions, are (1) the adoption of digital technologies, with their implications to reskilling and upskilling existing employees; and (2) cyber threats. One risk appears in six of the regions' top five risks for 2034: succession challenges and talent acquisition and retention. Finally, one risk appears in four top five lists: the rapid speed of disruptive innovation.

There are noticeable differences in views about risks around the globe, which is especially important for multinational organisations to consider.

FIGURE 29A

North America HQ Organisations — 2024

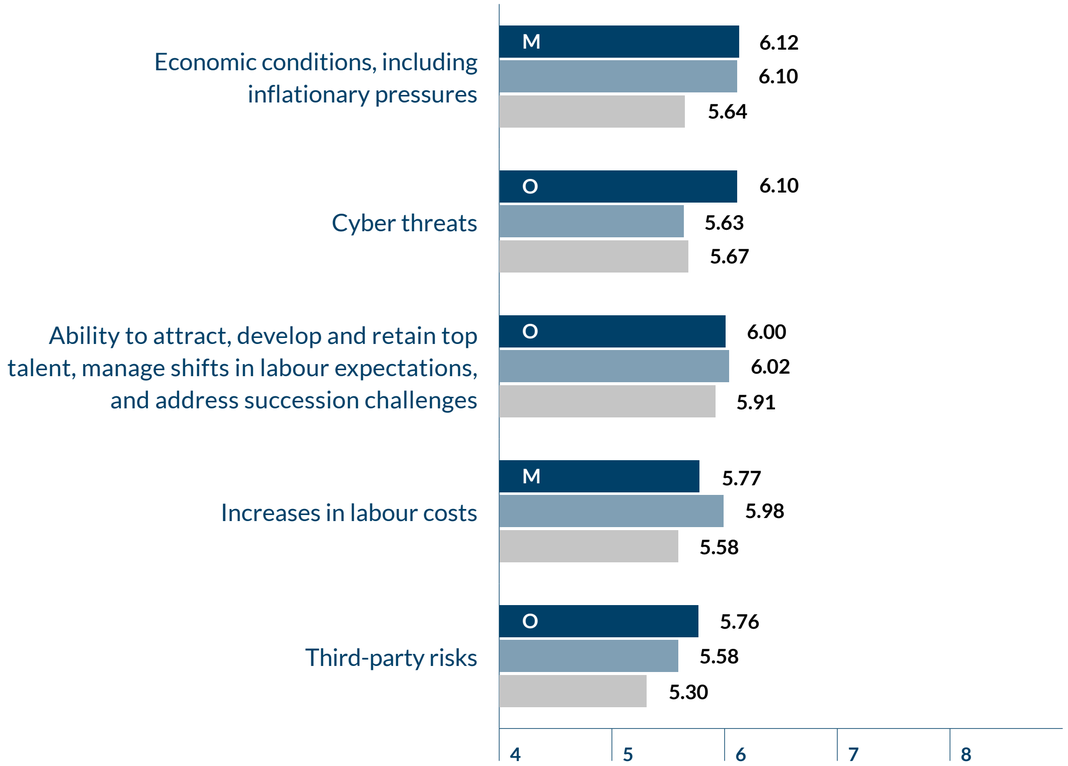
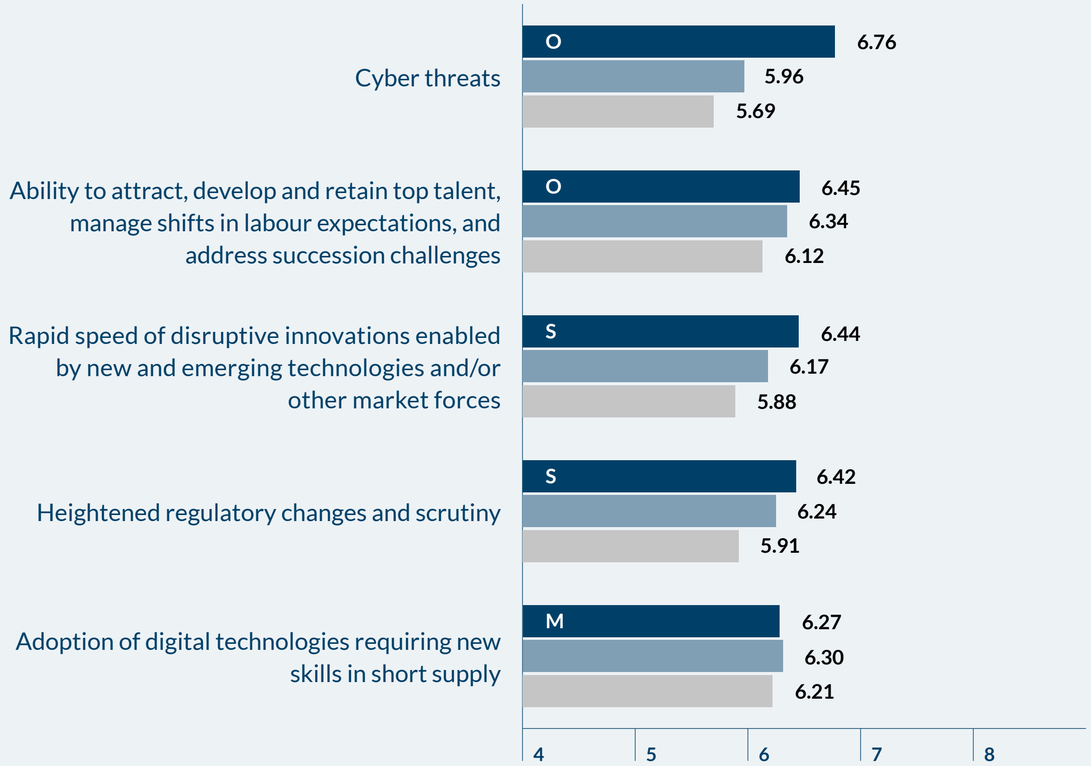


FIGURE 29B

North America HQ Organisations — 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.

FIGURE 30A

Europe HQ Organisations — 2024

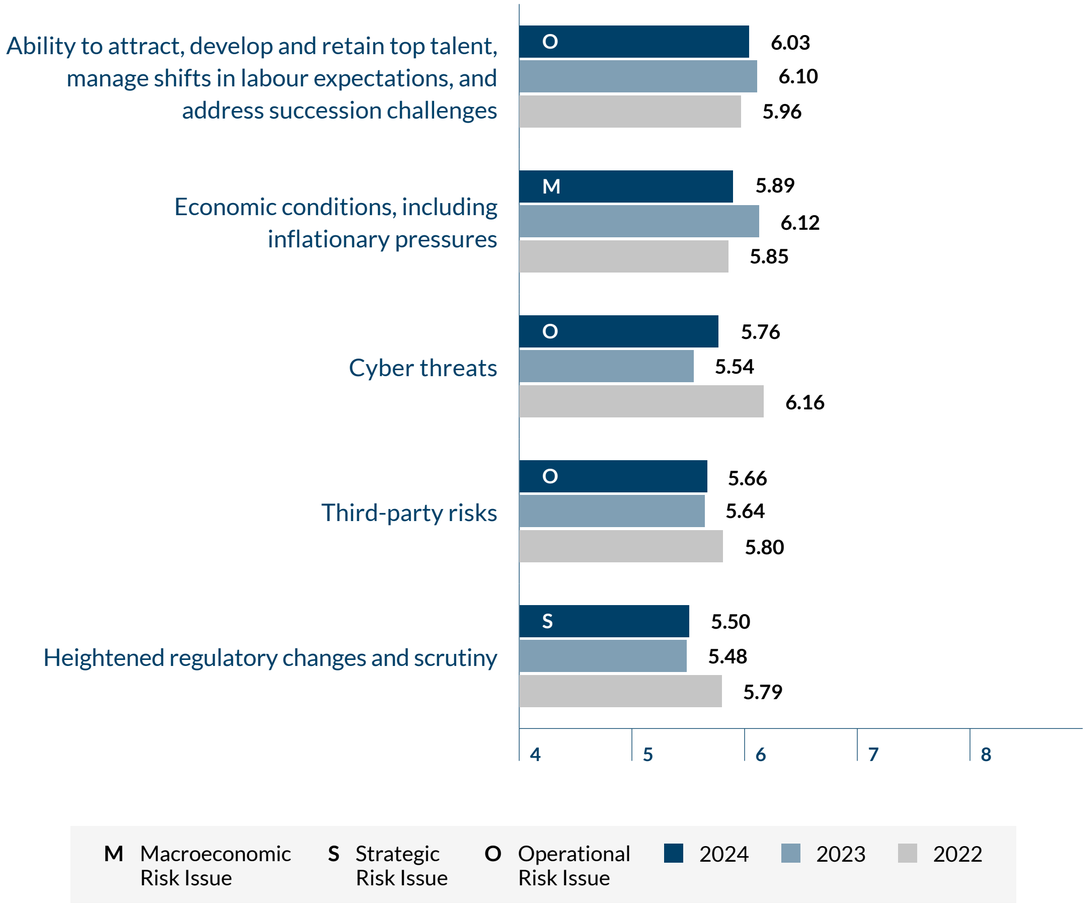
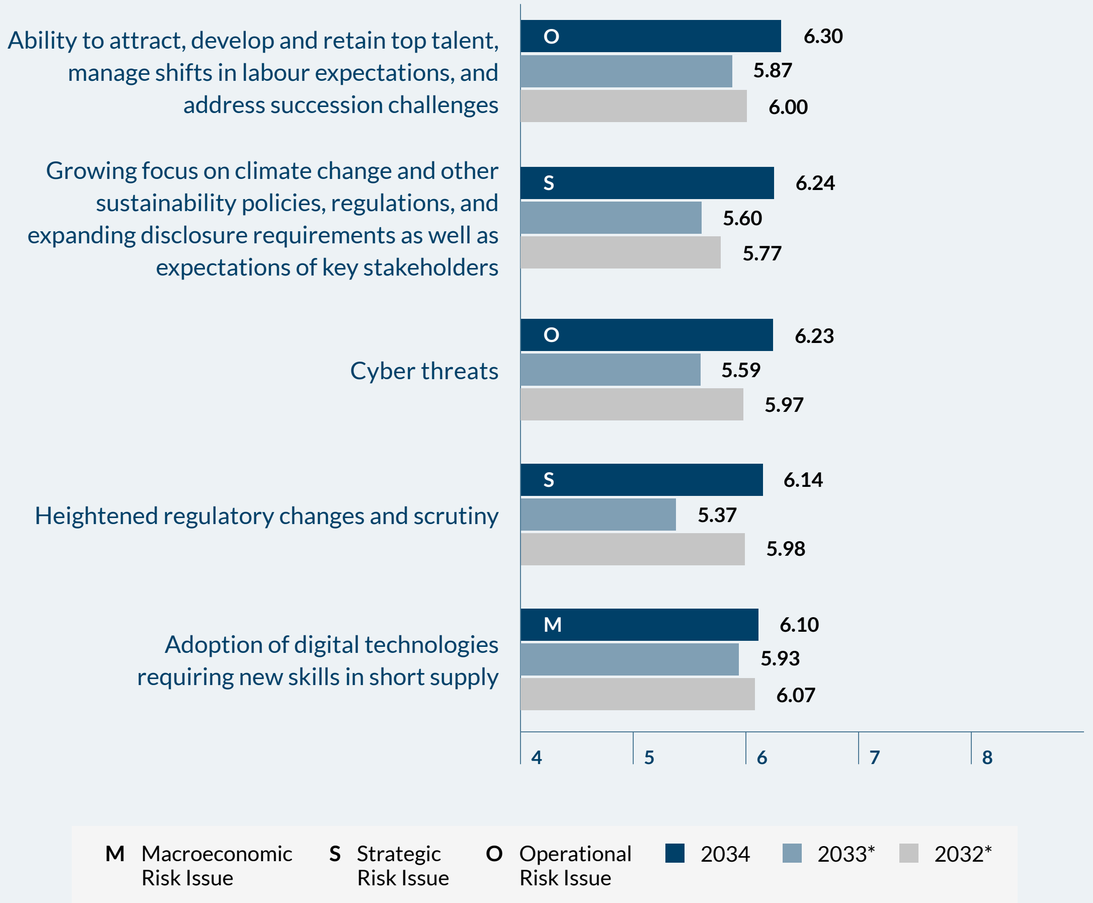


FIGURE 30B

Europe HQ Organisations — 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.

FIGURE 31A

Australia/New Zealand HQ Organisations — 2024

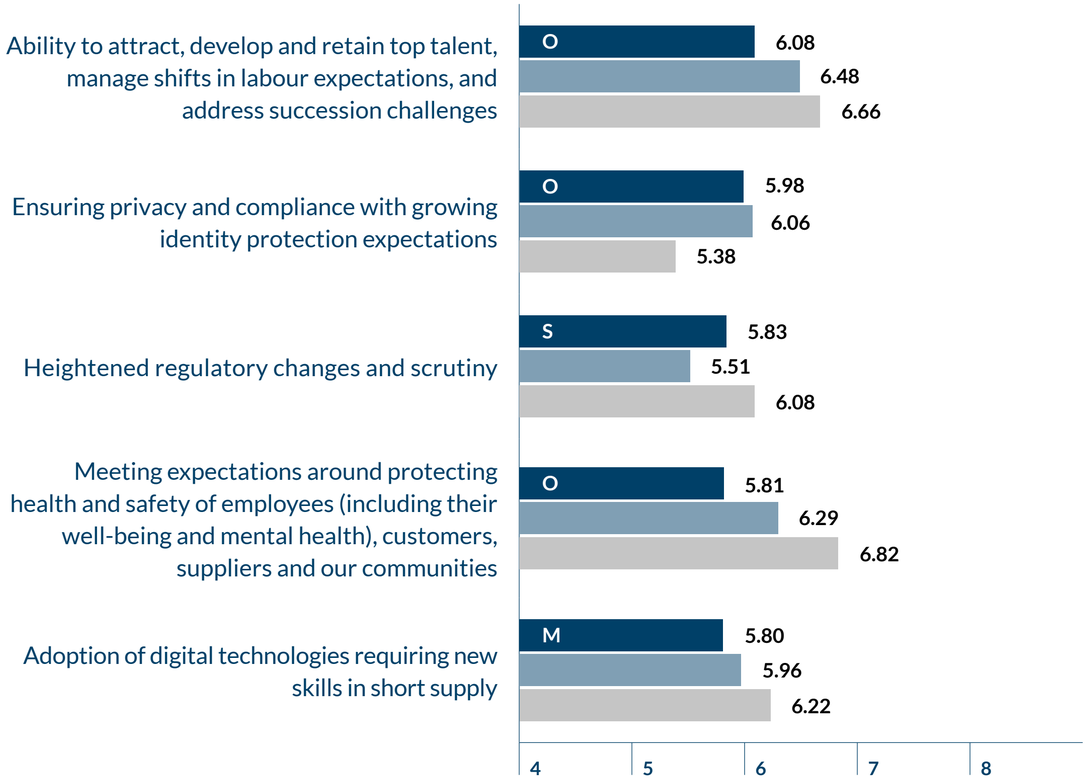
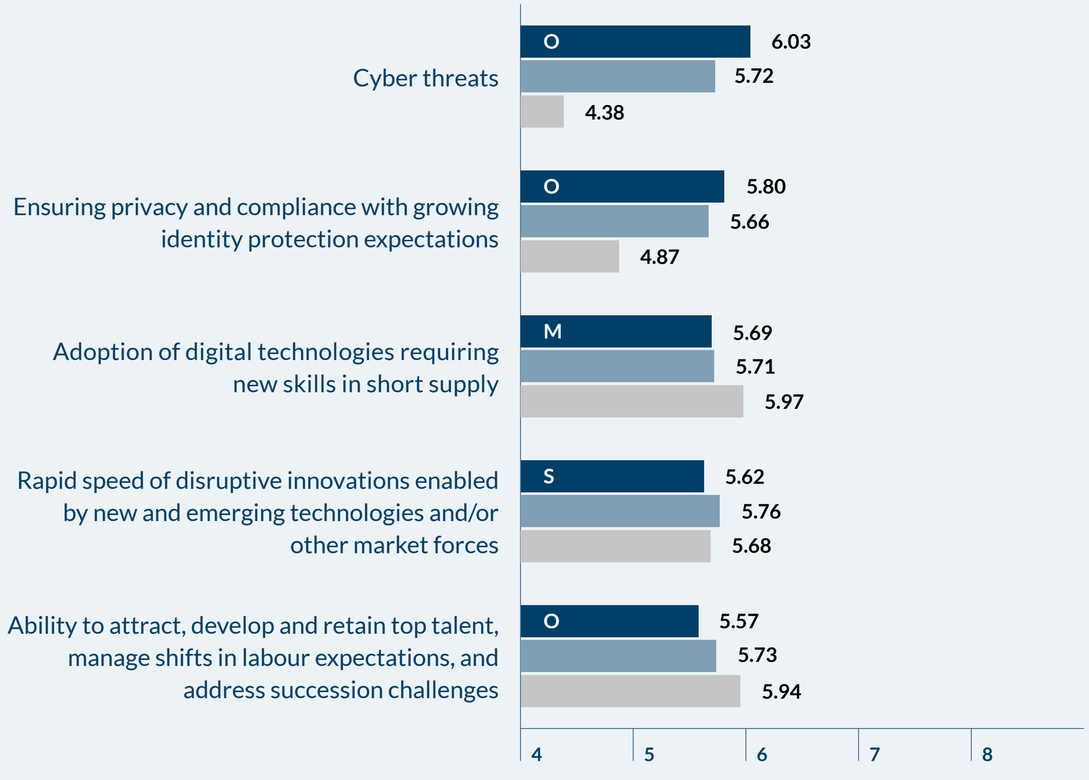


FIGURE 31B

Australia/New Zealand HQ Organisations — 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.

FIGURE 32A

Asia HQ Organisations — 2024

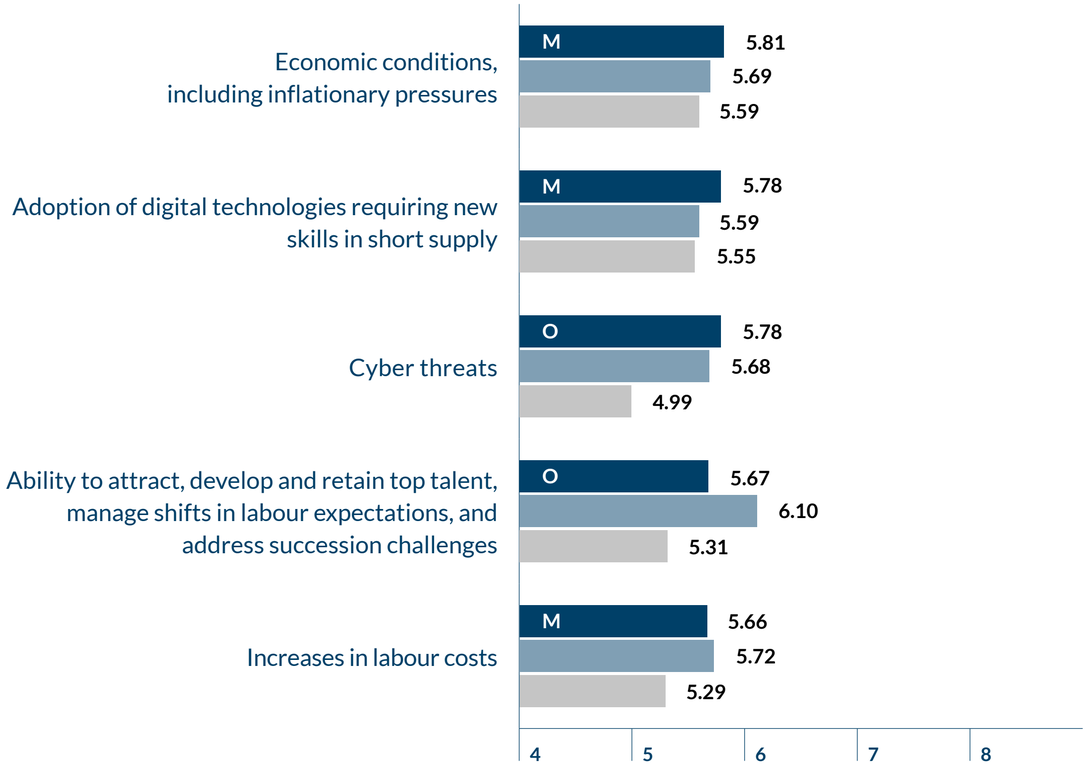
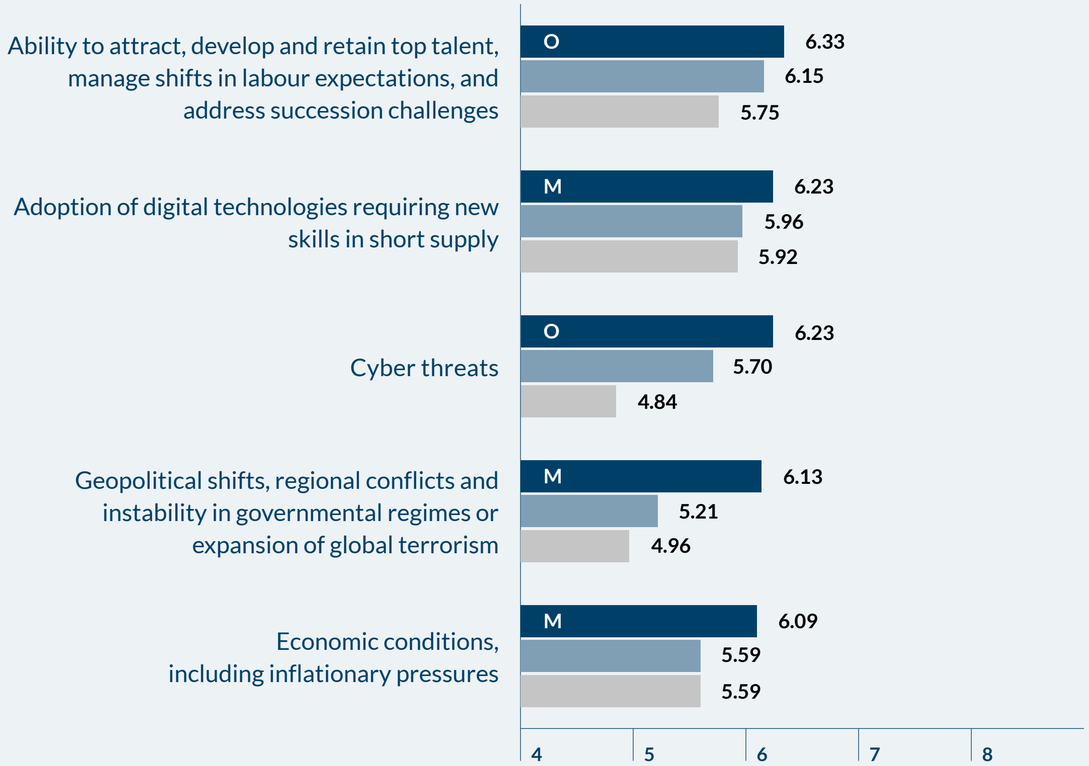


FIGURE 32B

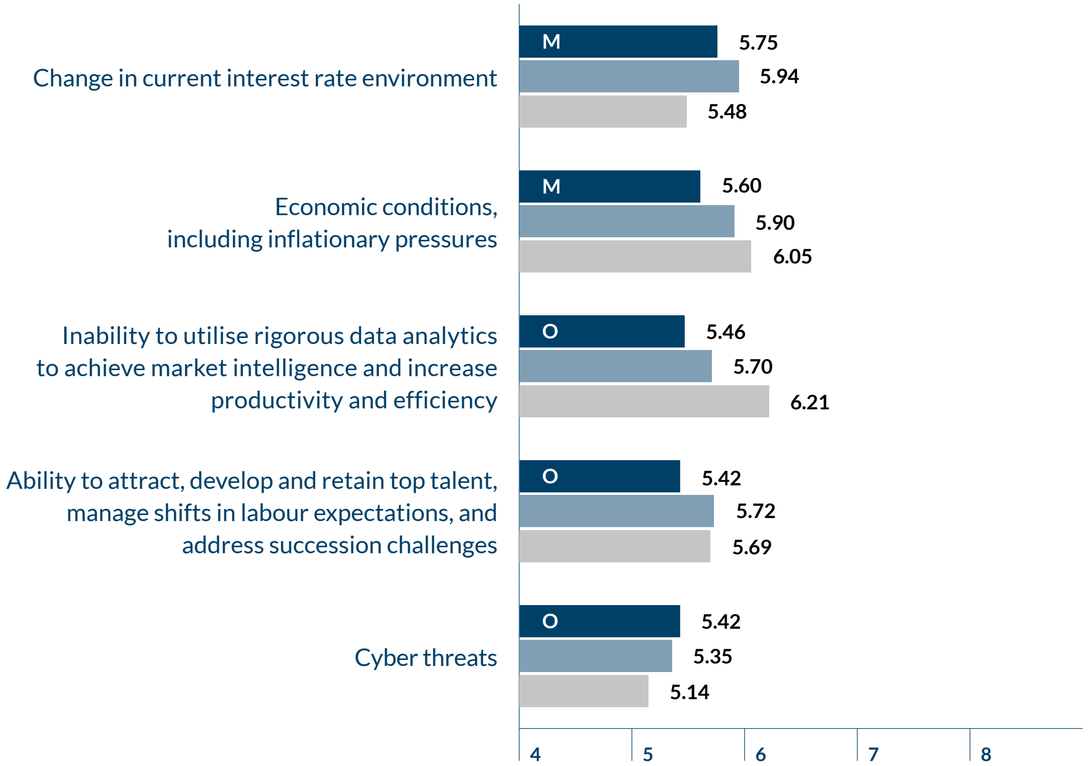
Asia HQ Organisations — 2034



* 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.

FIGURE 33A

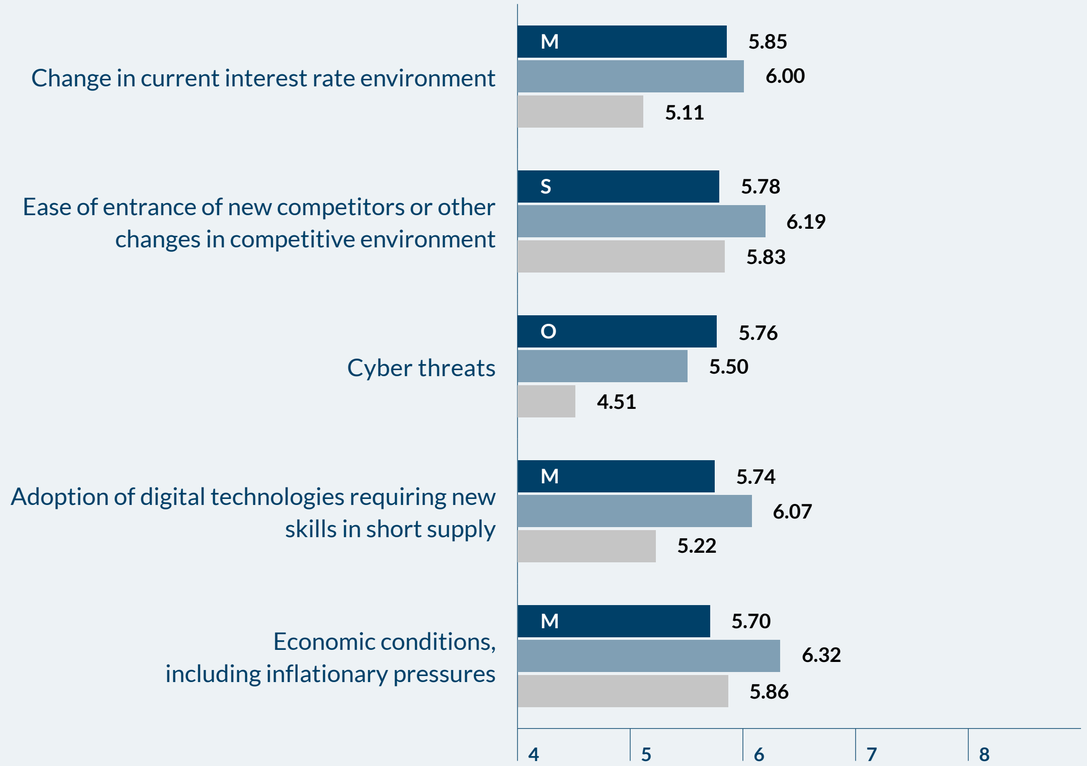
Latin America HQ Organisations — 2024



M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue 2024 2023 2022

FIGURE 33B

Latin America HQ Organisations — 2034



M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue 2034 2033* 2032*

* 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.

FIGURE 34A

Middle East HQ Organisations — 2024

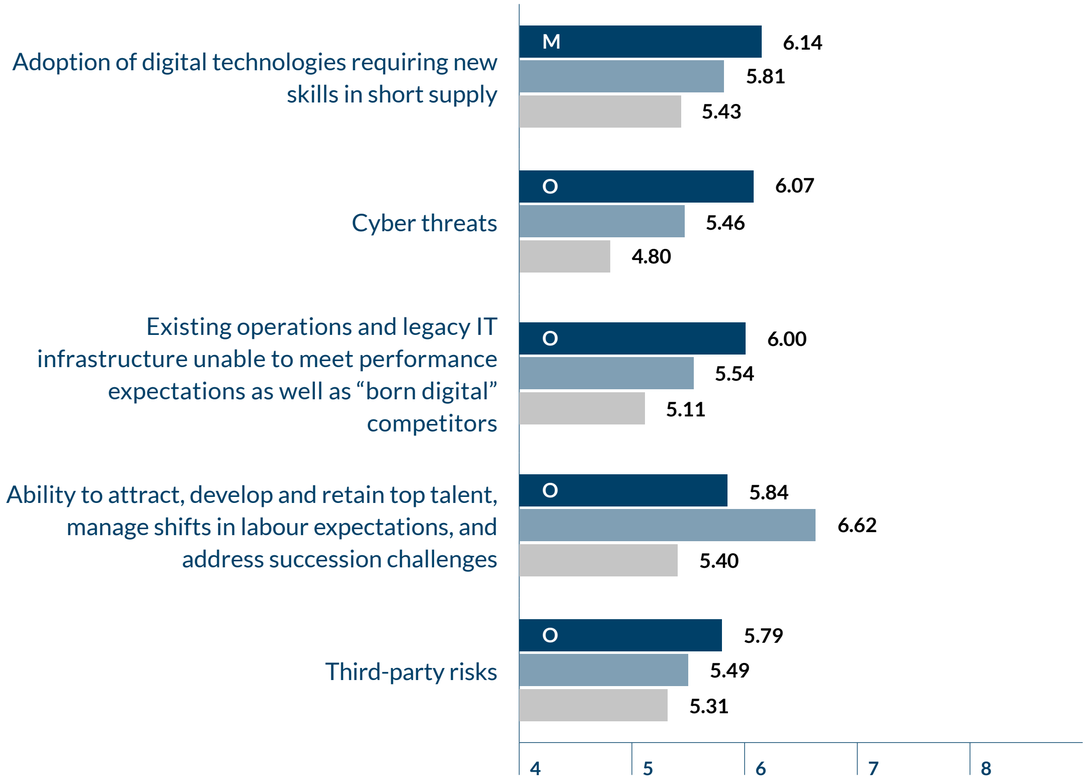
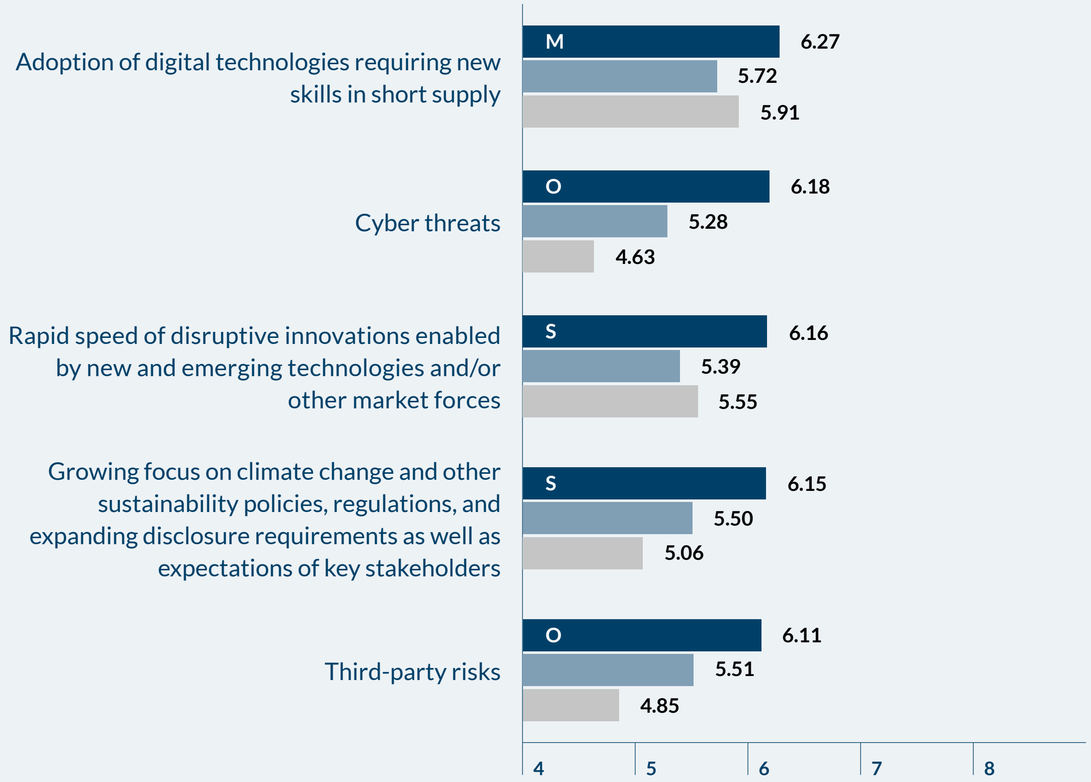


FIGURE 34B

Middle East HQ Organisations — 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.

FIGURE 35A

India HQ Organisations — 2024

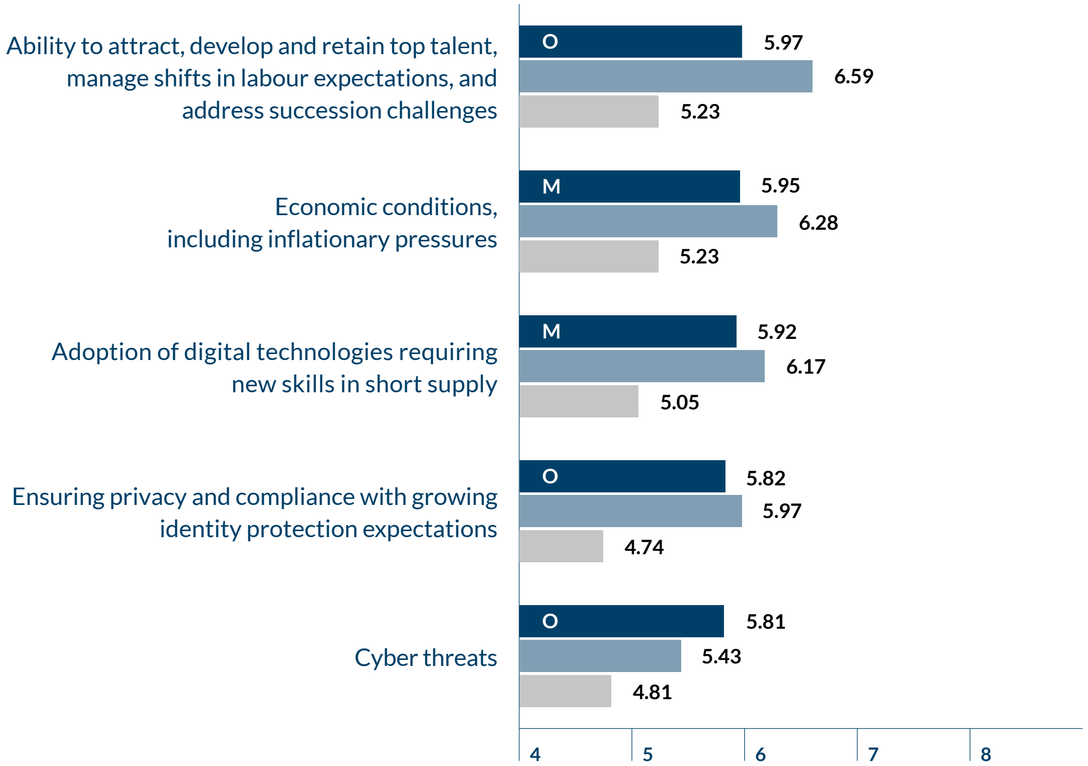
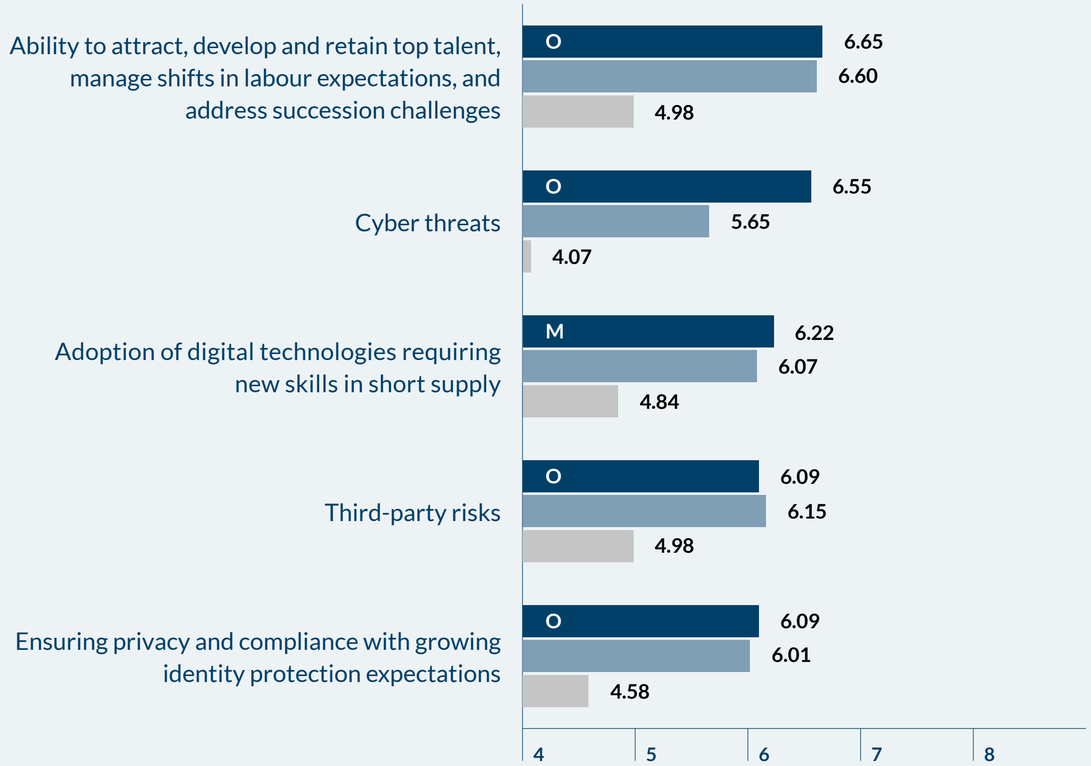


FIGURE 35B

India HQ Organisations — 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.

FIGURE 36A

Africa HQ Organisations — 2024

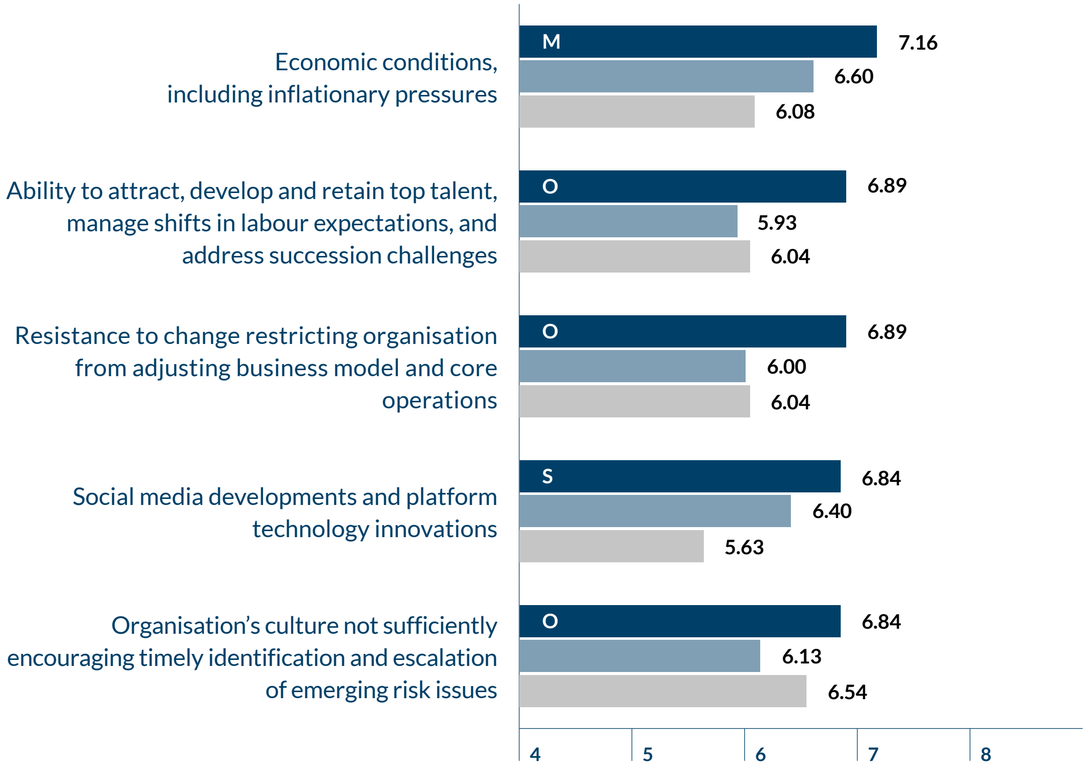
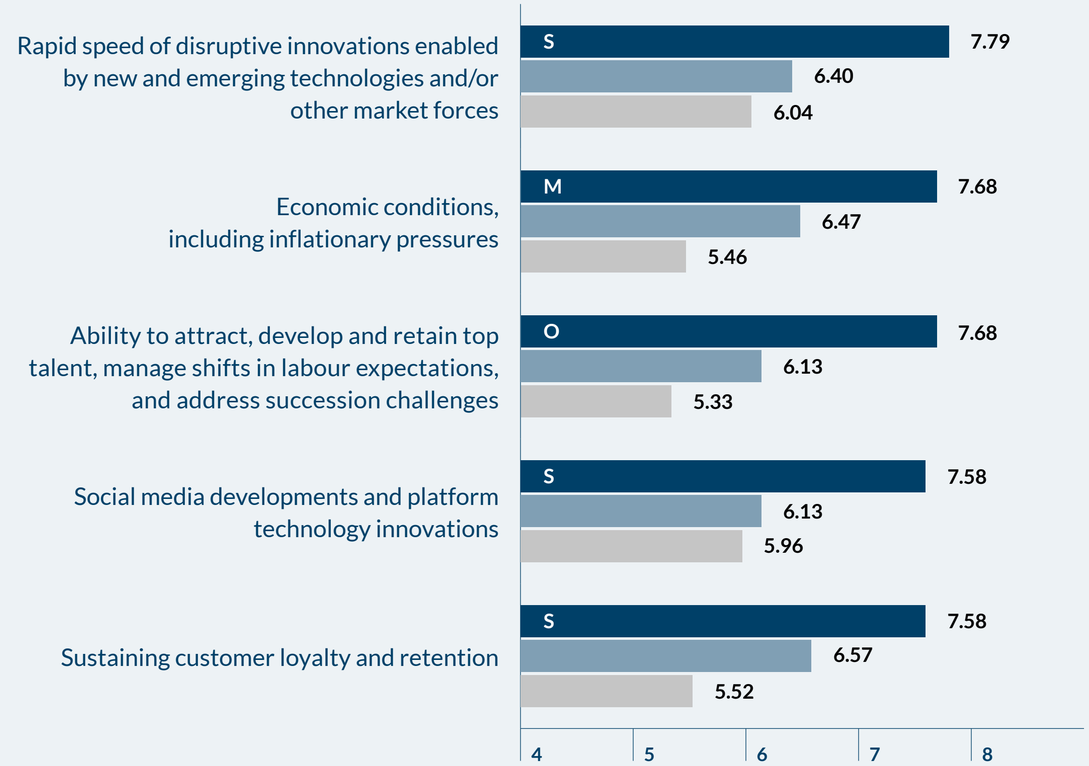


FIGURE 36B

Africa HQ Organisations — 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.

Analysis across public and non-public entities

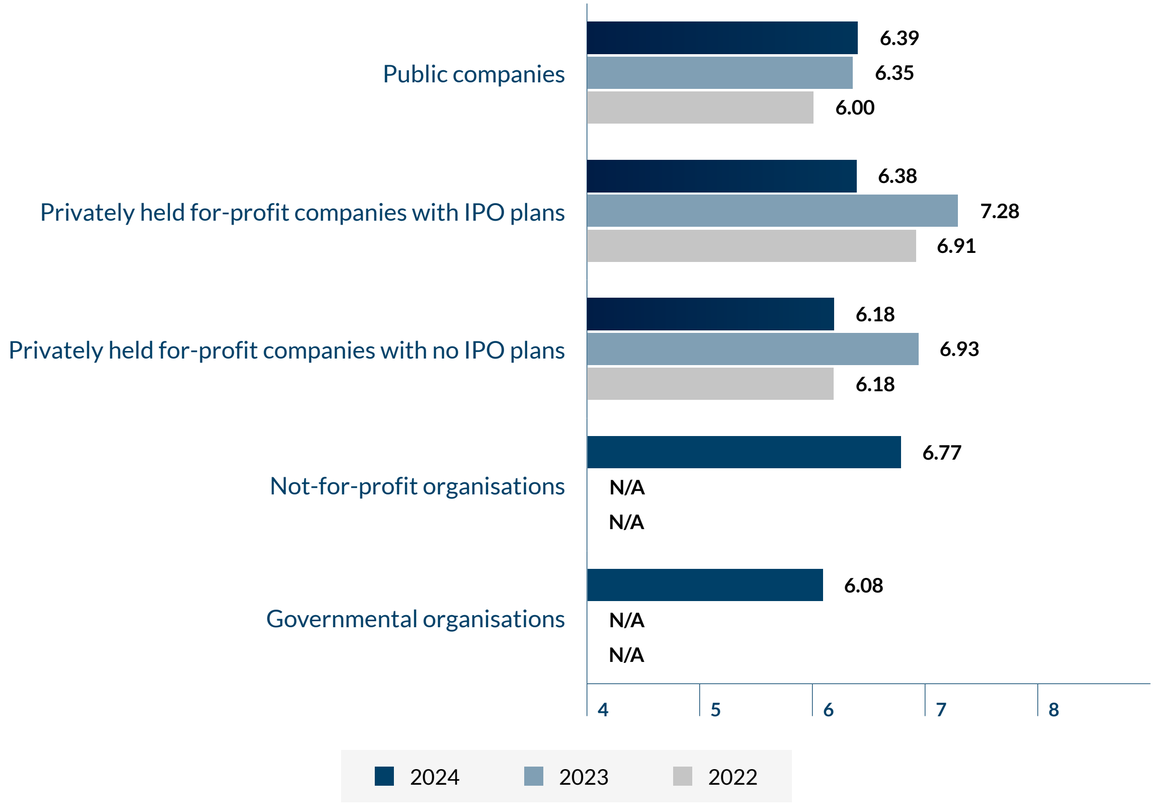
Participants in the survey represent five types of organisations: publicly traded companies (587 respondents), privately held for-profit entities with plans for an IPO (116 respondents), privately held for-profit entities with no plans for an IPO (269 respondents), not-for-profit organisations (100 respondents), and governmental organisations (71 respondents). For this year's report, we provide analyses of the separate responses we received from not-for-profit organisations and from governmental organisations.[23] In prior years we have combined these two into a single category.

We analyse responses across these five types of entities to determine whether different types of organisations rank-order risks differently. Similar to our analysis summarised earlier, we analyse responses about overall impressions of the magnitude and severity of risks across the five organisational type categories. Again, the scores in Figure 37 reflect responses to the question about the overall impression of the magnitude and severity of risks using a 10-point scale where 1 = "Extremely Low" and 10 = "Extremely High."

[23] Please note that in addition to this breakout of governmental organisations, we also have a breakout of government industry organisations presented earlier in our report. We distinguish these two groups as follows: Government industry organisations are those that function within a government at the national/federal, state or local level (e.g., a government agency). Government organisations may be entities that, while under the auspices of a government, operate or identify themselves as part of another industry (e.g., financial services, healthcare).

FIGURE 37

Overall, what is your impression of the magnitude and severity of risks your organisation will be facing with respect to achieving your performance goals over the next 12 months?



All five entity types agree that the overall magnitude and severity of risks are of a "Significant Impact" level in 2024, with not-for-profit organisations exhibiting especially elevated risk concerns.

Figures 38-42 highlight the top five risks identified by each type of organisation.

2024 risk concerns

The top five risks across the five groups are relatively consistent. All five groups rank succession and talent acquisition and retention among their top three risks. In addition, economic conditions in markets currently served appear in four of the top five risk summaries, as does the risk associated with cyber threats. Third-party risks appear in the top five for three of the five groups.

Macroeconomic and operational risk concerns dominate the top five risk issues for all organisations. Only public companies include a strategic risk in their top five — the risk associated with regulatory change and enhanced regulatory scrutiny. No other groups include any strategic risk issues in their top five risk concerns for 2024. For all but public companies, at least three of the top five risk concerns are operational risk issues.

As noted, within the privately held for-profit category, we captured responses from participants who classified their respective organisations as either "preparing to become publicly held" or "no current plans to become publicly held." Both groups share concerns over economic conditions (ranked first for both) and succession and talent acquisition and retention risks (ranked second for both). As well, both groups rate the risk associated with third parties as their fifth-highest risk concern. For private companies with no plans for an IPO, cyber threats and risks associated with digital technologies and reskilling their labour force appropriately round out their top five. For private companies with IPO plans, risks associated with organisational culture impacted by the work environment and privacy concerns complete their top five risk concerns for 2024.

2034 risk issues

The risk of cyber threats is top of mind, appearing in each group's top five risks list and ranked as the number one risk issue for public entities, private entities with IPO plans and governmental organisations. There are also significant concerns about succession and talent challenges continuing into the next decade, with that risk issue appearing in four of the top five risk summaries for 2034. The adoption of digital technologies and its implications for reskilling and upskilling existing employees is also a top five risk concern for four of the five groups — only private companies with IPO plans failed to include this risk in their top five.

As well, rapid speed of disruptive innovations enabled by advanced technologies appears as a top five risk for all but private companies with IPO plans. These firms also exhibit the most variation in their risk concerns for 2034 relative to the other groups. Three of the top five risks for private companies with IPO plans appear only on their top five risks list. All five groups include at least two operational risks and three of the five include at least two strategic risks in their lists of top five risk issues looking out a decade.

FIGURE 38A

Public companies — 2024

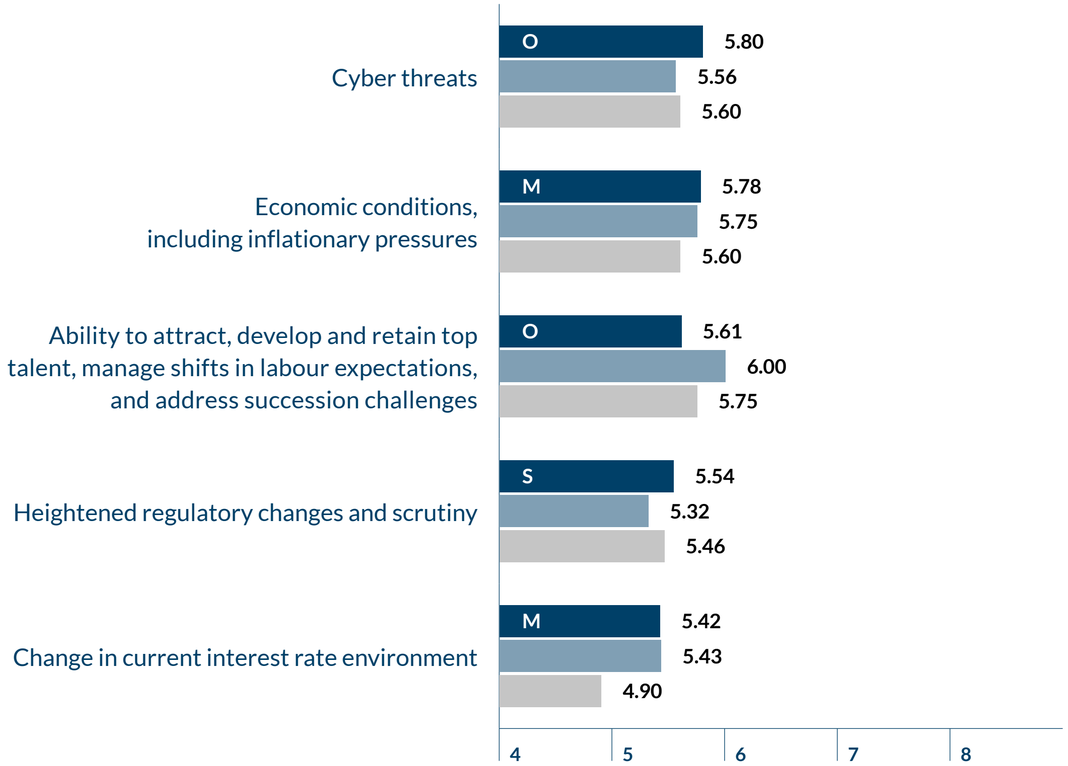
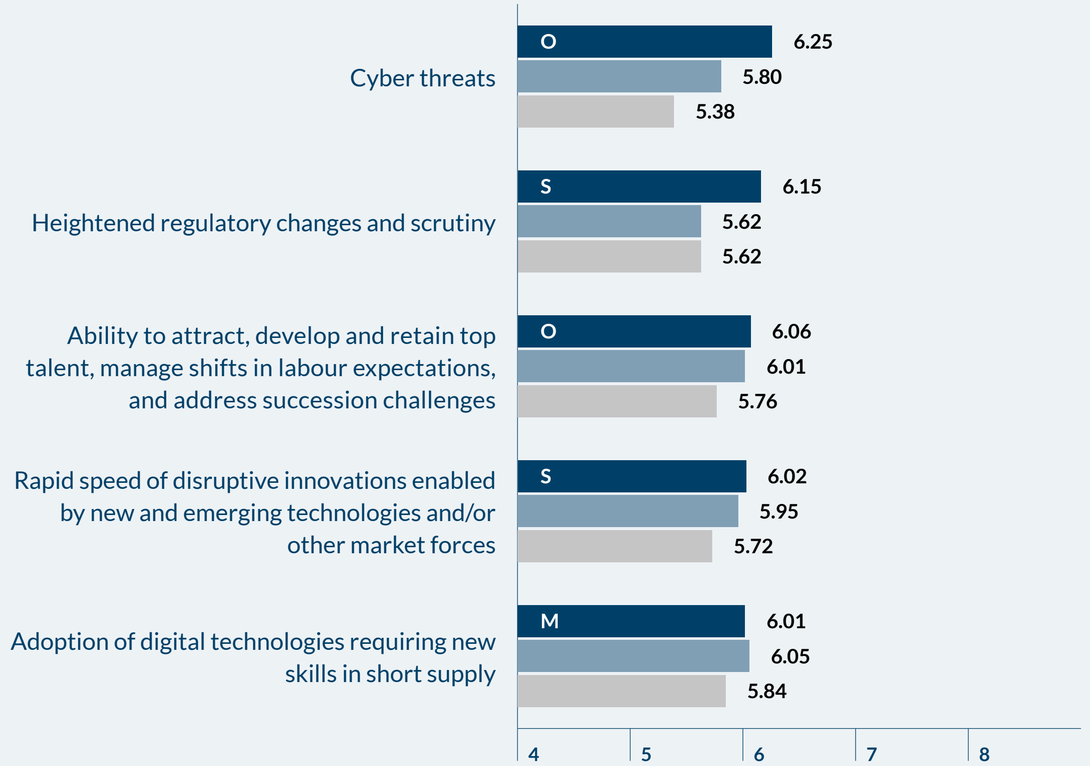


FIGURE 38B

Public companies — 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.

FIGURE 39A

Privately held for-profit companies with IPO plans — 2024

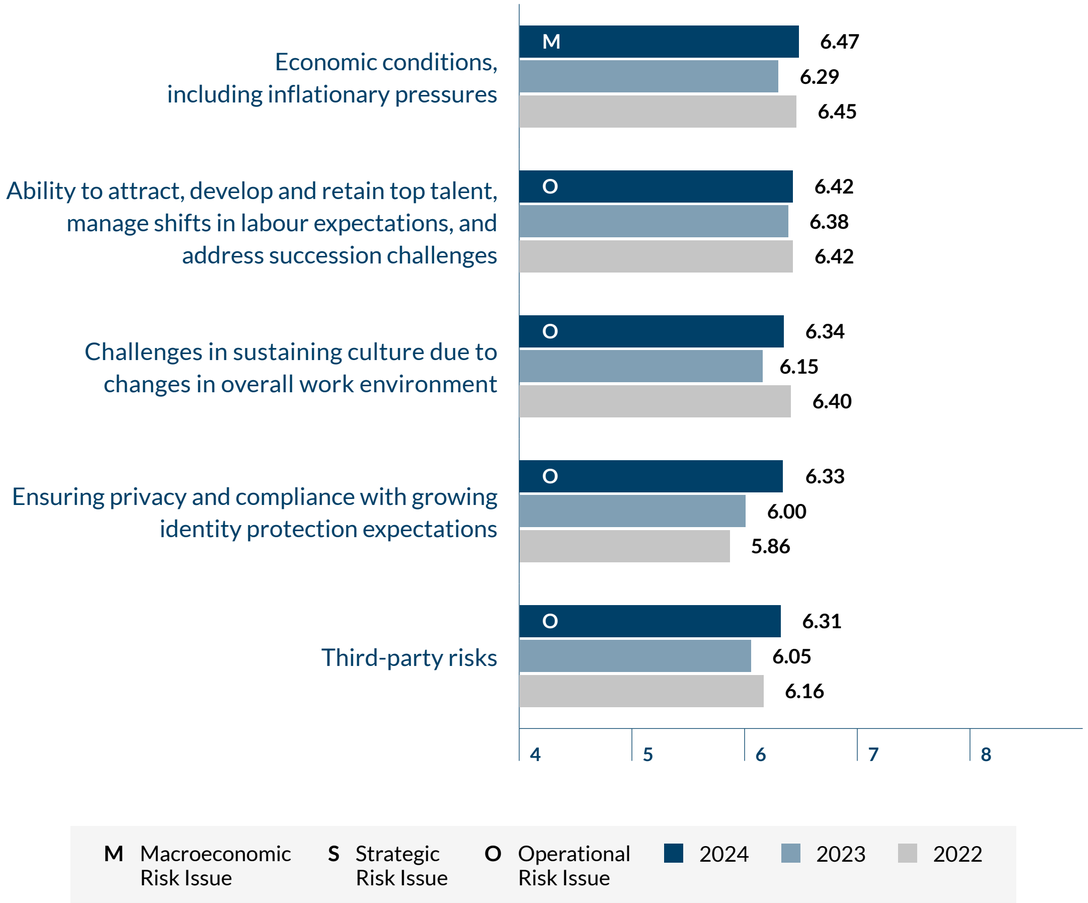
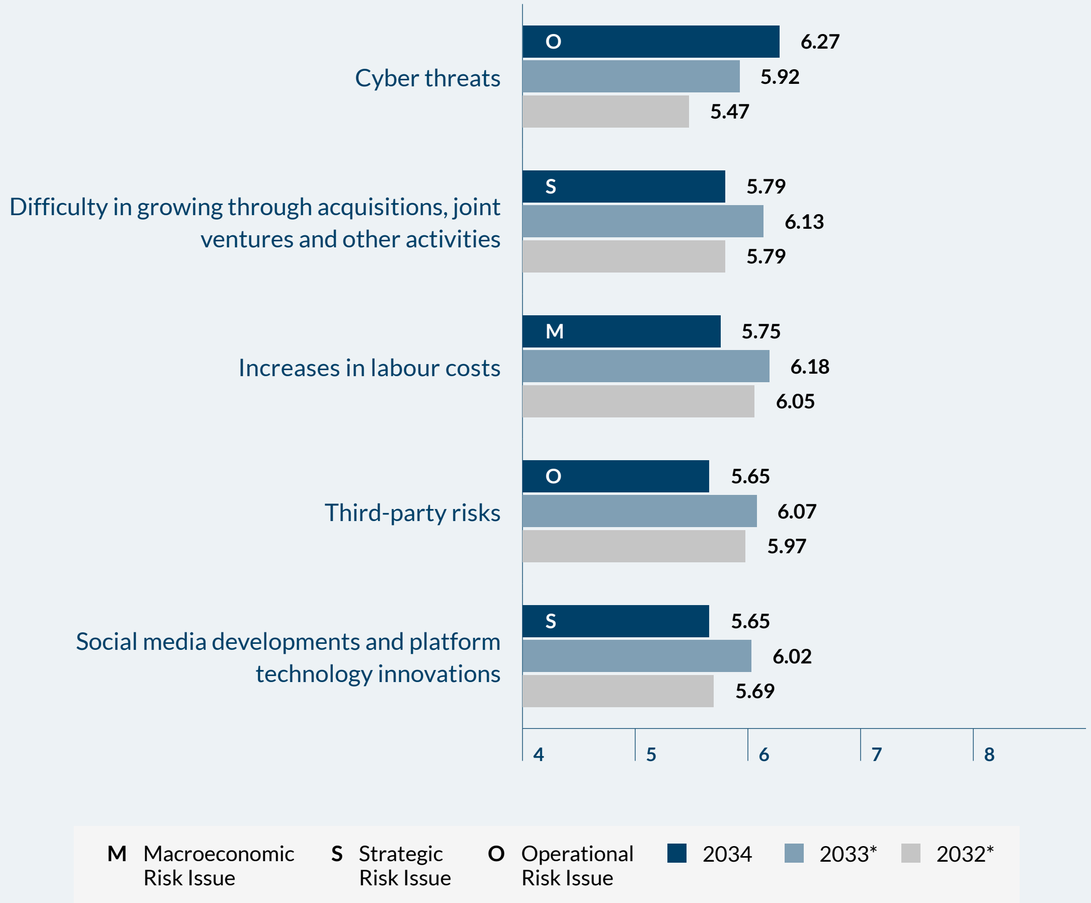


FIGURE 39B

Privately held for-profit companies with IPO plans — 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.

FIGURE 40A

Privately held for-profit companies with no IPO plans — 2024

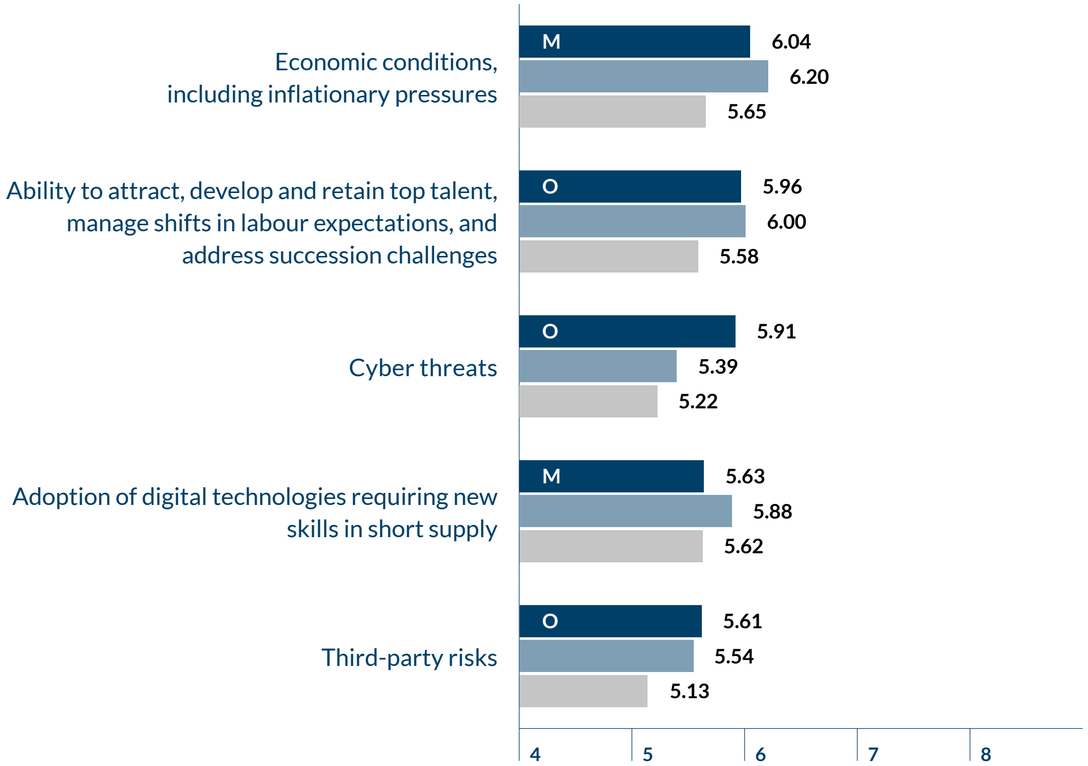
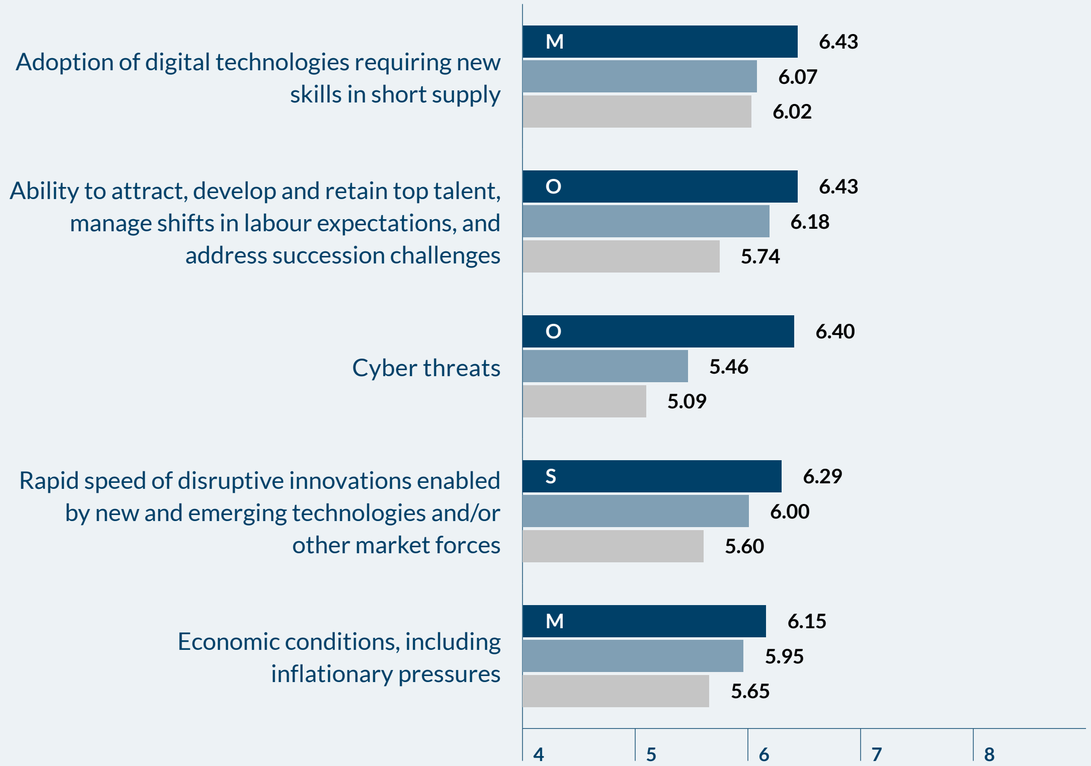


FIGURE 40B

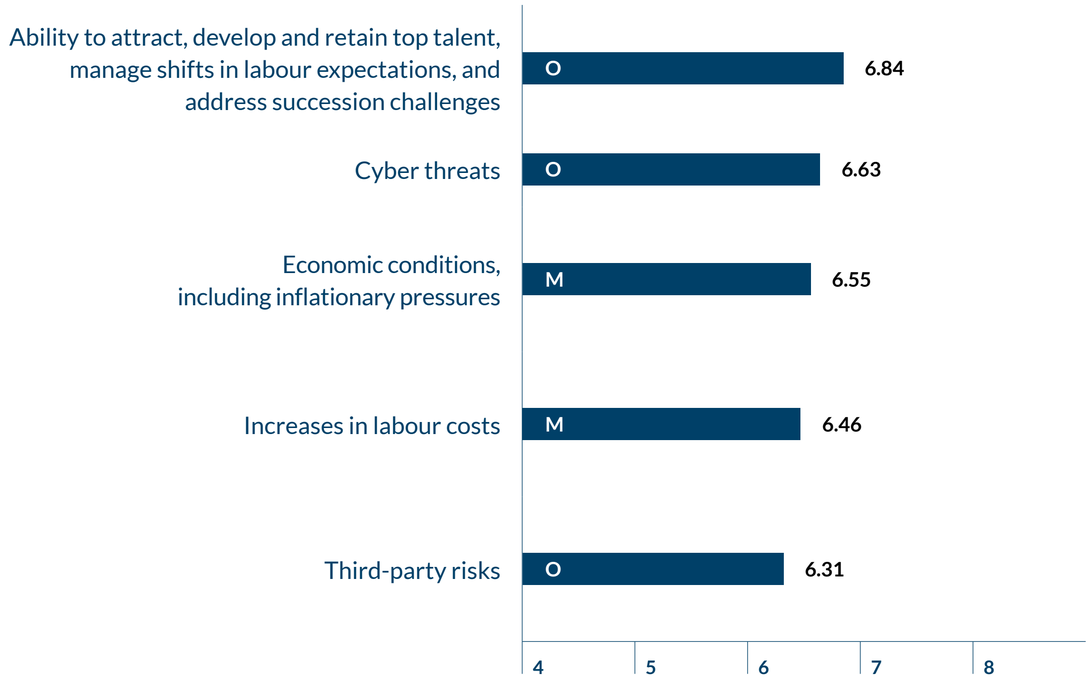
Privately held for-profit companies with no IPO plans — 2034



* 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.

FIGURE 41A

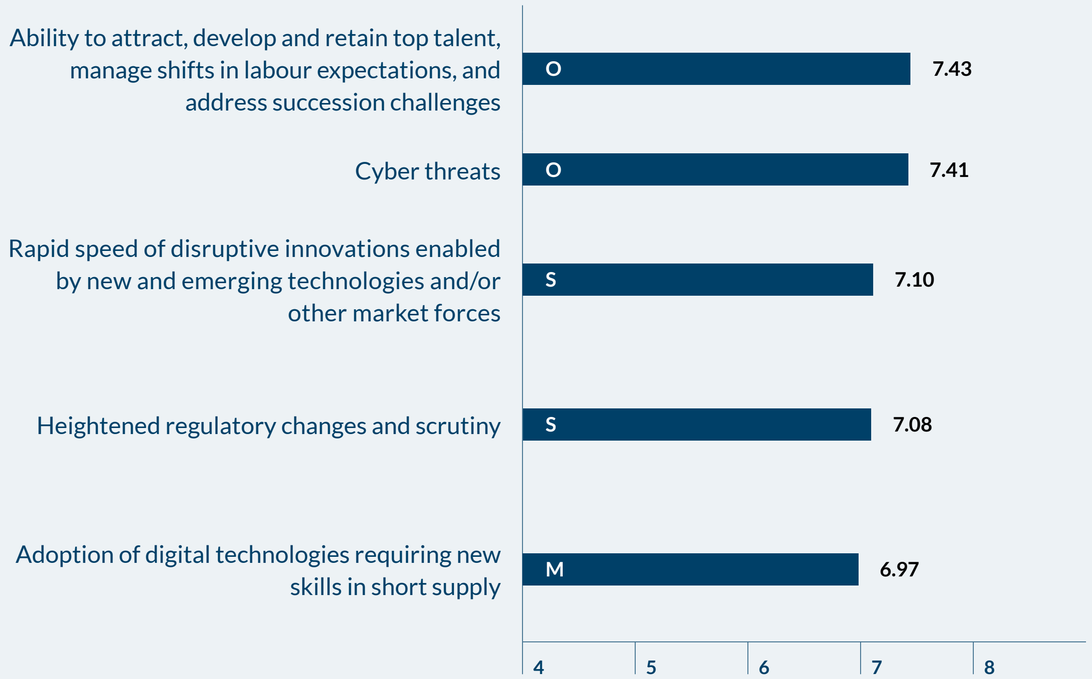
Not-for-profit organisations — 2024*



* For this year's survey, we have broken out governmental and not-for-profit organisations into separate groupings, whereas in our prior year survey reports we combined these two groups.

FIGURE 41B

Not-for-profit organisations — 2034*

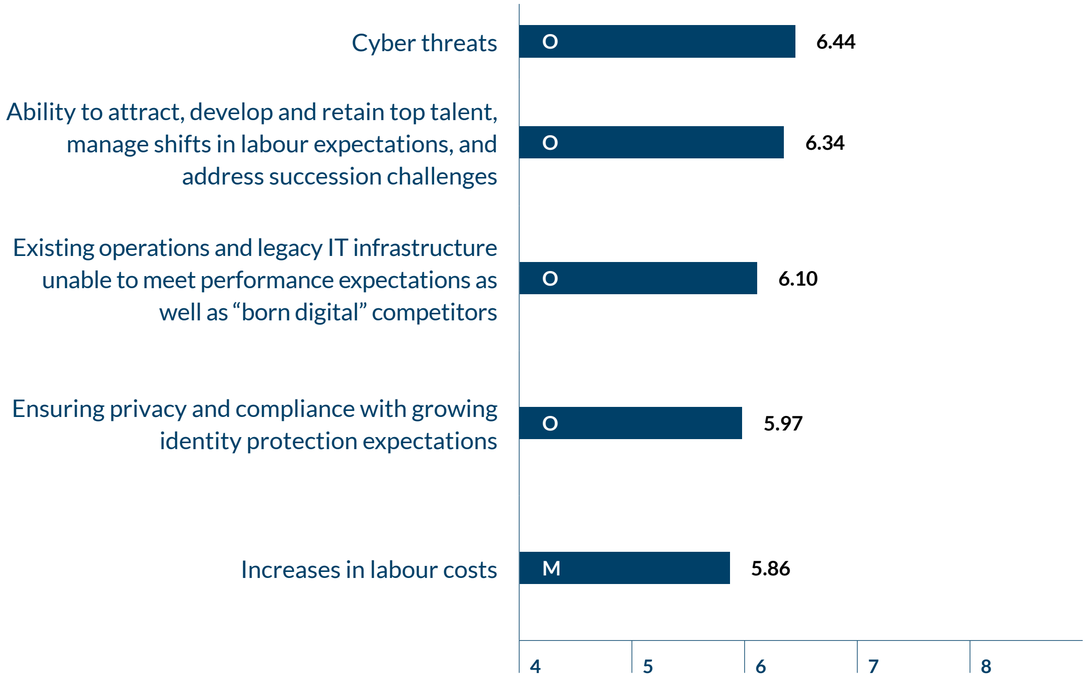


* For this year's survey, we have broken out governmental and not-for-profit organisations into separate groupings, whereas in our prior year survey reports we combined these two groups.

** 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.

FIGURE 42A

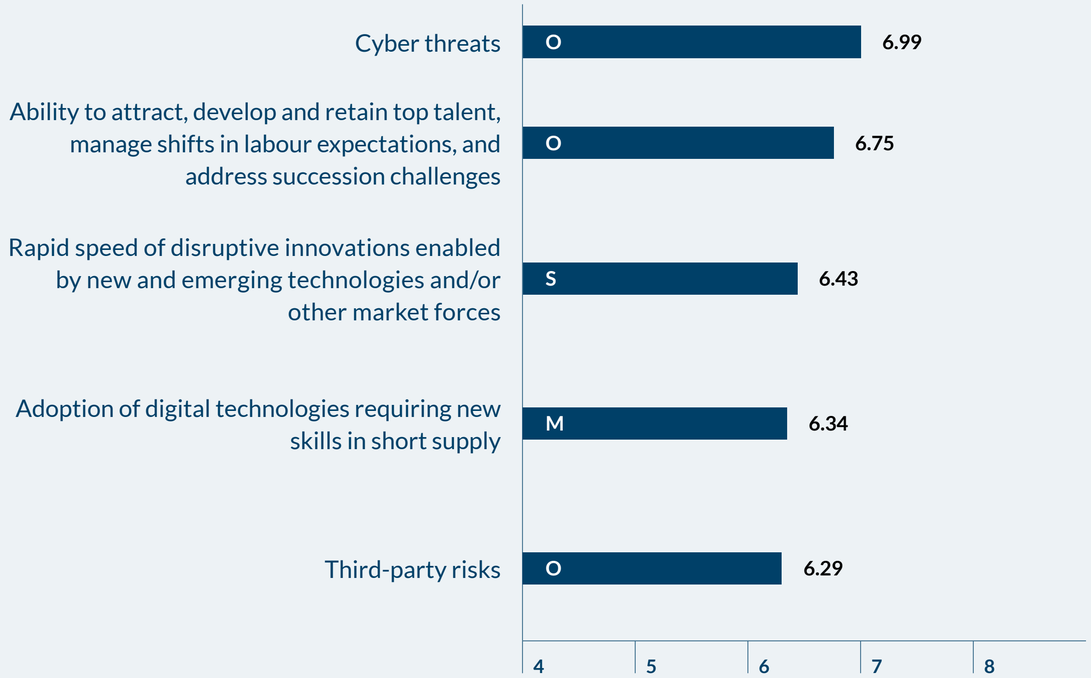
Governmental organisations — 2024*



* For this year's survey, we have broken out governmental and not-for-profit organisations into separate groupings, whereas in our prior year survey reports we combined these two groups.

FIGURE 42B

Governmental organisations — 2034*



* For this year's survey, we have broken out governmental and not-for-profit organisations into separate groupings, whereas in our prior year survey reports we combined these two groups.

** 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.

Responses to open-ended questions on major 2024 concerns

In our survey, we invited respondents to answer three open-ended questions seeking additional insights. After analysing the responses received, we elected to present those received on two of the three questions.

The first question we selected to include in this report asked:

Looking to 2024, are there developments or issues that present especially significant or out-weighted effects on your business?

The words portrayed in the word cloud on this page capture the essence of the responses received on the above question.

Interestingly, the focus of the responses is predominantly on significant change in the business and its operations as well as key drivers of change — regulations, cost structure, interest rates, cybersecurity, inflation, supply chains and the economy. The company's markets, customers and competition as well as the geopolitical environment, climate issues and labour markets were also mentioned. In addition, the responses address important enablers to managing change, e.g., strategy, data, technology, systems and information.

The above themes relate to a number of risks ranked highly in our overall survey results, as previously discussed in this report. Without question, leaders have a lot on their minds as they approach 2024.

The second question we selected asked:

Are there any risk issues that are of particular significance to your organisation or the overall risk environment for 2024 and/or 2034?

The words portrayed in the word cloud on this page capture the essence of the responses received on this question.

The responses point to a number of near-term and long-term themes highlighted in this report. With respect to the long term, that cybersecurity is displayed prominently is no surprise as it was the top risk concern looking out 10 years. The responses also refer to technology, people, leadership, the economy, the industry, regulations, employees, competition, customers, operations, and the geopolitical and political environments — issues that relate either directly or indirectly to the top 10 risks for 2034. Reference is also made to climate issues which is the 13th-rated risk long-term. Interestingly, there are references to population, government, DEI and supply sources.

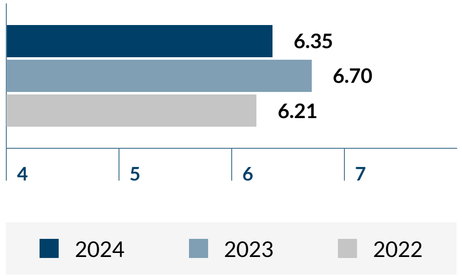
These responses, once again, reflect wide-ranging issues and challenges that are top of mind for leaders across the globe.

Plans to deploy resources to enhance risk management capabilities

Recall that we asked respondents about their overall impression of the perceived magnitude and severity of risks to be faced in 2024. (Note that we did not ask participants to consider this for 2034.) As illustrated in Figure 43, the average overall response indicates a perceived decrease in the nature of the overall risk environment, with an average score of 6.35 in 2024 relative to 6.70 in 2023 but higher than the 6.21 reported in 2022. Also, last year we added a new category of responses received from CHROs, who rated the overall magnitude and severity of risks as 8.10 in 2023, as compared to the CHRO assessment of 6.02 for 2024. We believe that the decline in their ratings from 2023 to 2024 has contributed to the lower overall assessment in magnitude and severity of 6.70 in 2023 to 6.35 in 2024 for the full sample.

FIGURE 43

Magnitude/severity of risks



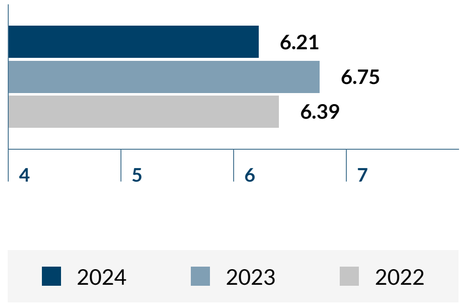
We also asked executives to provide insights into whether their organisation plans to devote additional resources to improve risk management capabilities over the next 12 months. We used a 10-point scale, whereby 1 signifies "Extremely Unlikely to Make Changes" and 10 signifies "Extremely Likely to Make Changes."

Consistent with the decrease in the perception of the risk environment, respondents indicate a lower likelihood of deploying more resources to risk management in 2024 relative to 2023 (and 2022), as reflected by Figure 44.

Even with this decline, there continues to be a need to invest in more robust risk management capabilities. The decline is perhaps partially explained by the significant increase in investment that has occurred over the past few years, largely driven by the need to improve organisational resilience pursuant to navigating the challenges posed by the pandemic. That experience highlighted the need for preparedness and agility as well as demonstrated that companies can innovate relatively quickly.

FIGURE 44

Likely to devote additional resources to risk management

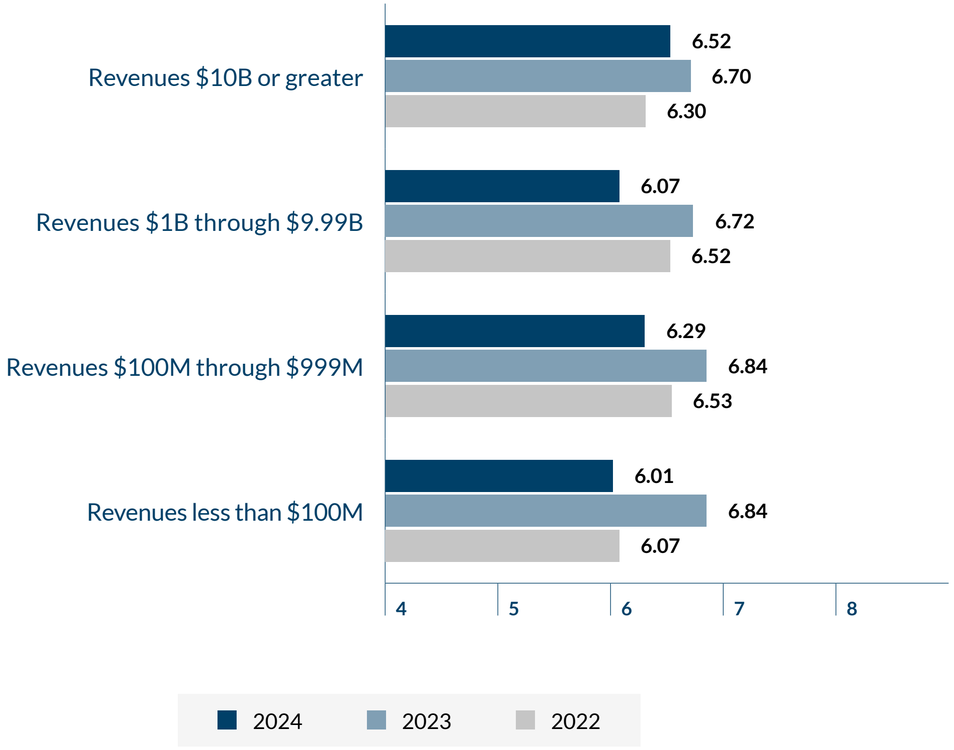


Organisation size analysis

We also analyse responses to these questions across different sizes of organisations. This year we observe that all organisations indicate a decrease in the likelihood of greater investment in risk management resources. As discussed above for the full sample, we believe this result is largely driven by increased investment in prior years, leaving little room for continued increases. It is worth noting that the largest organisations are more likely to devote additional resources to risk management relative to smaller-sized organisations.

FIGURE 45

How likely or unlikely is it that your organisation will devote additional time and/or resources to enhance its risk management capabilities over the next 12 months?

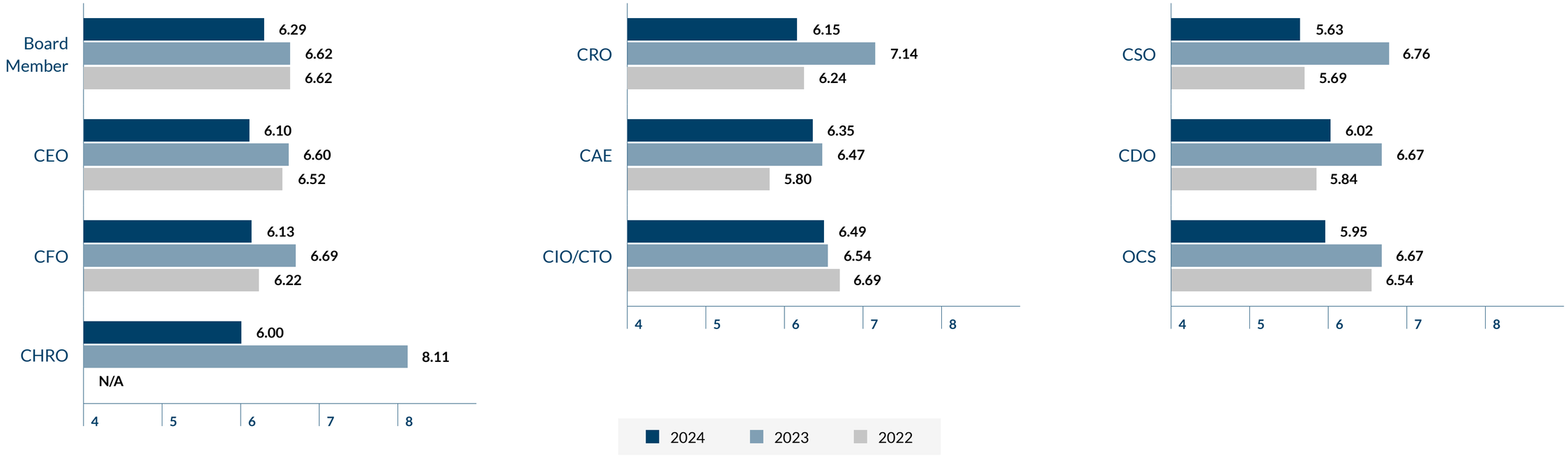


Respondent position analysis

Interestingly, all positions indicate a decrease in the likelihood of committing enhanced resources to risk management capabilities in 2024. Our new group added last year, CHROs, exhibits the largest reduction of likelihood of increased investment in the coming year. CIO/CTOs signal the greatest desire to devote additional resources to risk management relative to all other executive positions.

FIGURE 46

How likely or unlikely is it that your organisation will devote additional time and/or resources to enhance its risk management capabilities over the next 12 months?

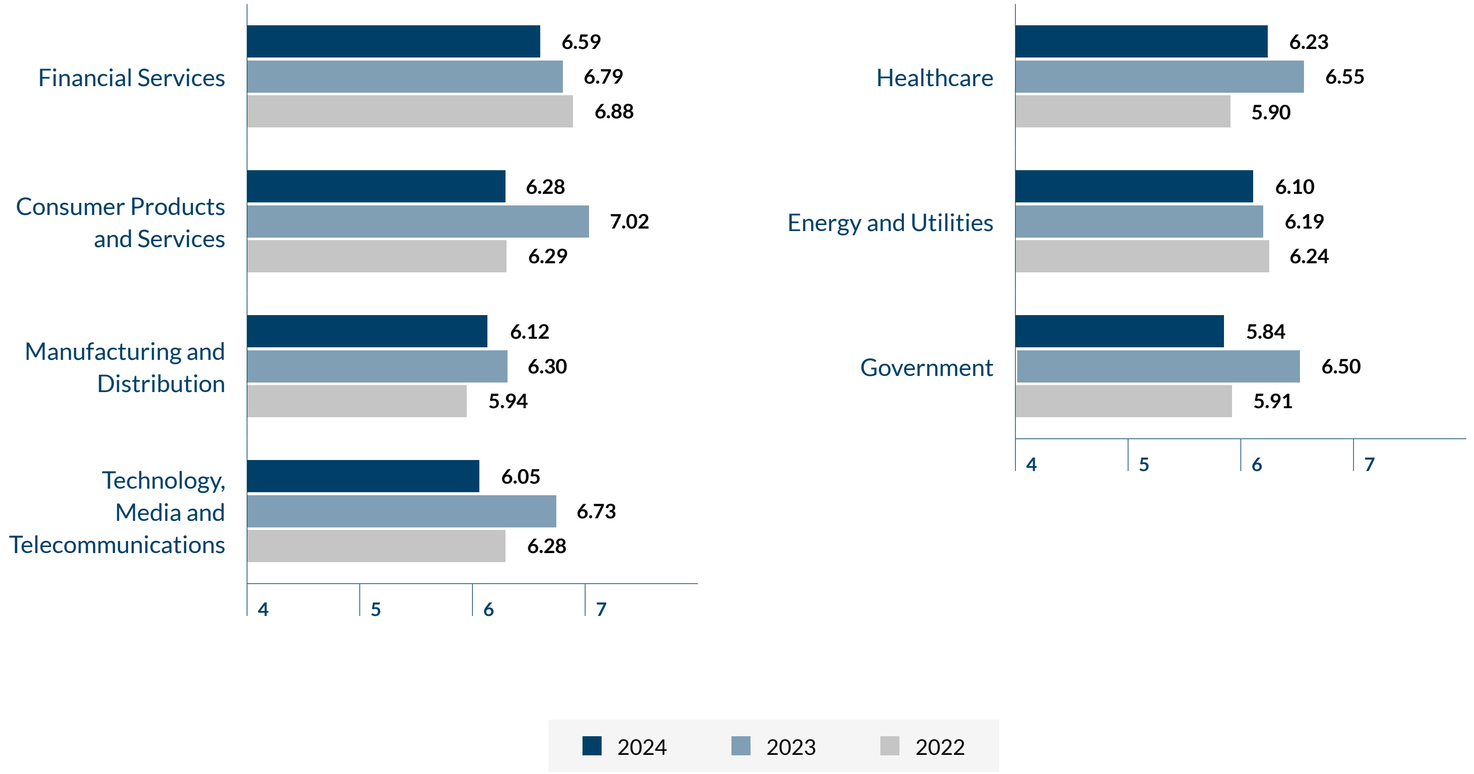


Industry analysis

All of our industry groups expect less investment in risk management capabilities in 2024 relative to 2023. This may simply reflect the increased investments already made in prior years, as noted previously. The Financial Services industry group leads in both absolute terms for 2024 (6.59) and in the magnitude of the decrease from 2023 expectations, which is relatively small (from 6.79 in 2023). The Consumer Products and Services industry group indicates the largest decrease in the level of likely investment in risk management capabilities in 2024 relative to 2023.

FIGURE 47

How likely or unlikely is it that your organisation will devote additional time and/or resources to enhance its risk management capabilities over the next 12 months?

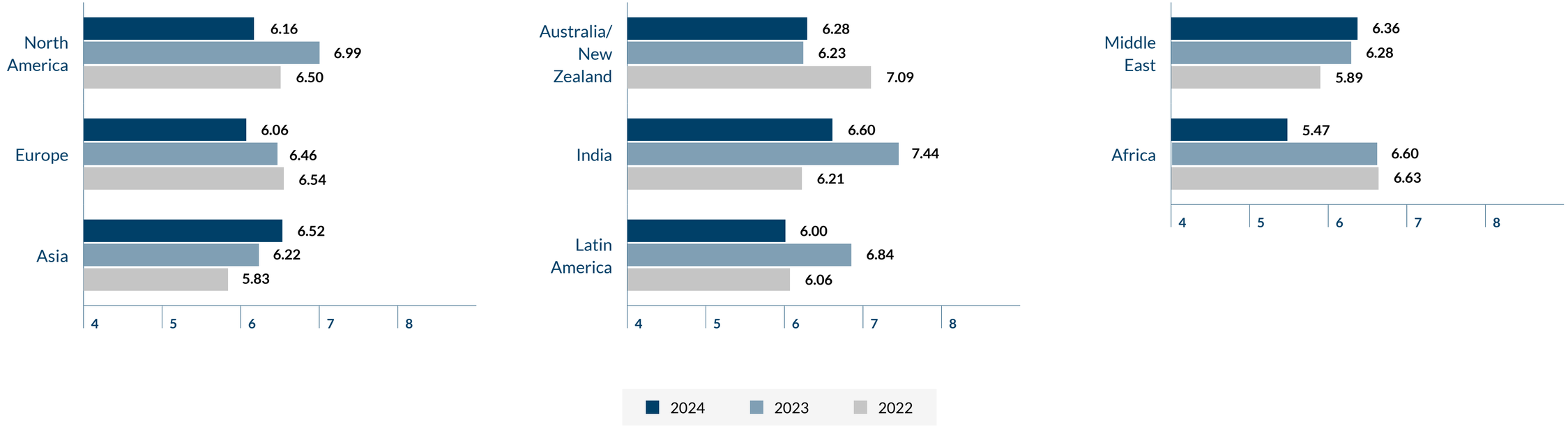


Geographic region analysis

Organisations with headquarters based in Asia, Australia/New Zealand, and the Middle East are the only regions that indicate an increased likelihood that they will devote additional resources to risk management in 2024, with all signalling a modest increase relative to 2023. The other five geographic regions we study all report a reduced likelihood of additional investment in risk management capabilities as compared to the 2023 results, perhaps caused by the increased investments they forecasted for 2023 in our prior year report.

FIGURE 48

How likely or unlikely is it that your organisation will devote additional time and/or resources to enhance its risk management capabilities over the next 12 months?

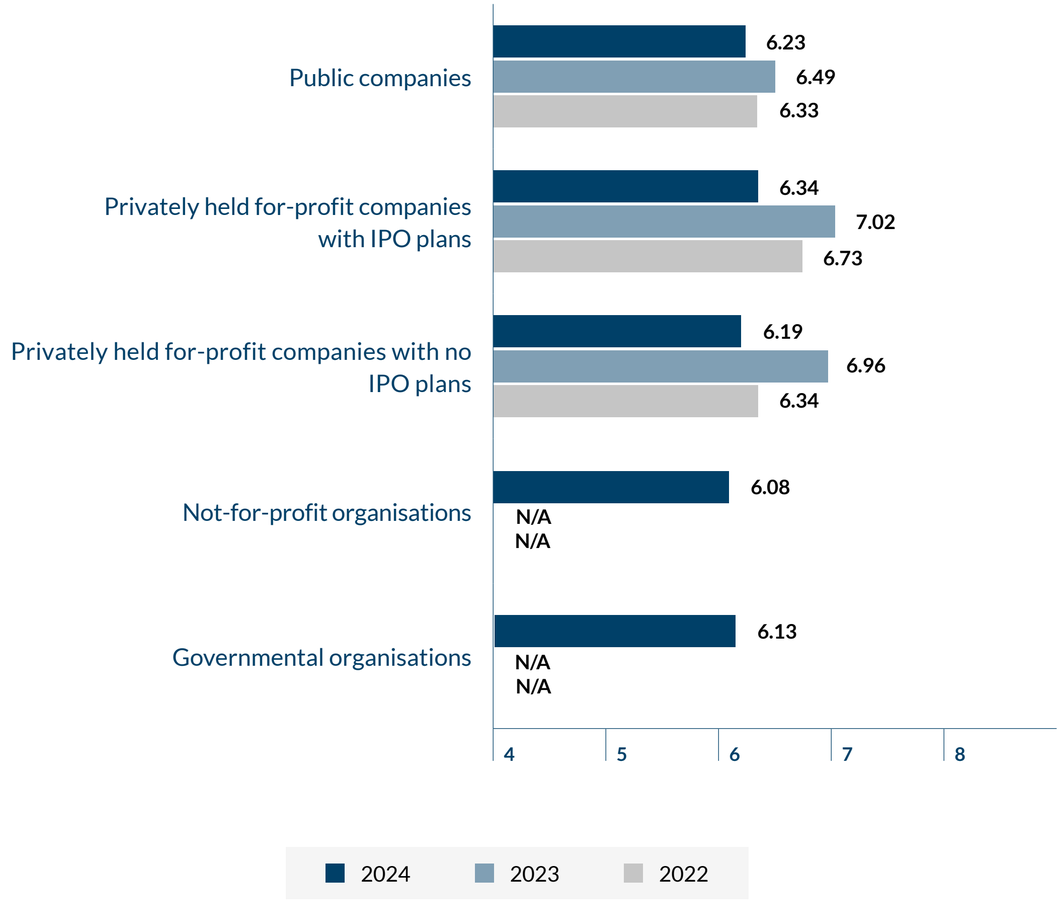


Organisation type analysis

For the three groups where we have prior year data for comparison, all indicate lower levels of likelihood that they will invest more time and resources in building out their risk management infrastructure in 2024 relative to 2023 (and 2022 as well). Not-for-profit and governmental organisations indicate similar likelihoods of additional investment in 2024 (6.13 for governmental organisations and 6.08 for not-for-profits).

FIGURE 49

How likely or unlikely is it that your organisation will devote additional time and/or resources to enhance its risk management capabilities over the next 12 months?



Evaluating an organisation's approach to risk oversight

This report provides insights from 1,143 board members and executives about risks that are likely to affect their organisations in the short term (over the next 12 months) and over the next decade (2034). Our respondents reveal that the scope of global risks has become more varied, and the number of different risks rated as top risk concerns is only growing in nature and type. There are noticeable shifts in what comprise the top risks for 2024 relative to last year, with many of those risks having a lingering impact that may extend a decade or more, reminding executives that risks are constantly emerging. In addition, the interrelated nature of the top risks noted in this year's survey makes for risk profiles that are nuanced and complex to manage.

Ongoing events continue to present major challenges for the next 12 months. The level of uncertainty in today's marketplace is rapidly evolving and presenting new risks that many previously thought were unimaginable. The ever-changing risk landscape and the overall perceived magnitude and severity of risks should prompt boards and senior executives to scrutinise closely the approaches their organisations use to keep an eye on risks emerging around the corner.

Unfortunately, some organisations continue to manage risks the way they have for many years, even though the profile of risks is evolving and the frequency and velocity of unexpected, disruptive events increase. As business transforms because of the rapidly advancing digital economy, game-changing innovations such as generative AI, and shifting geopolitical conditions, the risk profile is most certainly not yesterday's risks. A focus on financial and compliance risks using static analogue-age tools without any conception of the organisation's risk appetite leaves decision-makers across the organisation to their own devices. Soon those organisations may realise, once it's too late, that their level of investment in risk management and willingness to engage in robust tools to identify, manage and monitor risk are inadequate.

The focus today is on agility and resilience as much as it is on prevention and detection. It is about providing information for decision-making and enabling the organisation to be more anticipatory and prepared. Now may be an opportune time for boards and C-suites to examine closely how their organisations approach risk management and oversight in the digital age to pinpoint aspects requiring improvement.

The focus today is on agility and resilience as much as it is on prevention and detection. It is about providing information for decision-making and enabling the organisation to be more anticipatory and prepared.

In the interest of evaluating and improving risk management capabilities in light of the findings in this report, we offer executives and directors the following diagnostic questions to consider when evaluating their organisation's risk assessment and risk management processes. A "no" response to any of the following questions should be considered as a possible area of improvement. These diagnostic questions focus on assessments of these five fundamental elements of an effective risk management approach:

1. Robustness of risk management in light of the evolving business and geopolitical environment
2. Strategic positioning of the risk management process
3. Accountabilities for ownership of risks
4. Effectiveness of board communications about enterprisewide risks
5. Influence of leadership and culture on risk management

Specific assessment questions for each of these themes are provided below to help guide discussions among executives and boards to pinpoint opportunities for risk management enhancements.

Diagnostic theme: Assessing whether our risk management approach is sufficiently robust in light of our evolving business environment

Because risks are constantly changing, the risk management process needs to be repeatable, clearly defined and adequately resourced to ensure business leaders receive the information they need to stay abreast of emerging issues:

- Is the process supported by an effective, robust methodology that is definable, repeatable and understood by key stakeholders?
  - Does our approach to risk identification foster consideration of risks that may have a higher-level strategic impact and that may be triggered by external events or competitor actions that are beyond our organisation's control?
  - Does the process delineate the critical enterprise risks from the day-to-day risks of managing the business so we are able to focus the C-suite and boardroom dialogues on the risks that matter most?
  - Do we engage all the right stakeholders in the risk identification process?
  - Would most stakeholders describe our approach to risk management as one that is dynamic, engaging and insightful versus one that is stale, siloed across disparate functions in the organisation and/or requiring a refresh?
  - Is our approach appropriately balanced with respect to focusing on the macroeconomic, strategic, reputational, operational and compliance risks that matter?
  - How extensively do we evaluate the effectiveness of preparedness and response plans that are intended to either prevent risk events from occurring or reduce the impact of risk events should they occur?
- Is there a process for identifying emerging risks and does the risk identification process allow the board and management sufficient time to consider adequate response plans to these risks?
- Does our management dashboard system:
  - Include robust key risk indicators that help the leadership team monitor shifts in relevant external trends?
  - Cover the most critical enterprise risks?
  - Provide an effective early warning capability with action triggers and decision prompts that enable the organisation to act as an "early mover" in response to market opportunities and emerging risks?

Diagnostic theme: Assessing whether our risk focus is positioned to provide strategic value

Given the pace of change experienced in the industry and the relative riskiness and nature of the organisation's operations:

- Are we centring our focus on risks in the context of our organisation executing its strategy, achieving its business objectives, sustaining its operations, and preserving its brand image and reputation?
- Is our leadership's knowledge of top risks enhanced by the organisation's risk management process serving as a value-added input to the strategy-setting process?
- Does our risk management process consider extreme as well as plausible scenarios? Do we have meaningful discussions of potential "black swan" and "gray rhino" events?
- Does our risk management process consider a sufficient time horizon to pick up looming strategic and emerging risks (so called "gray rhinos"), e.g., the longer the horizon, the more likely new risk issues will present themselves?
- Is our focus on external risks linked to geopolitical shifts, emerging disruptive innovations and changes in macroeconomic factors?
- In our ongoing assessment of risk, do we consider the effects of changes in internal operations, personnel, processes, technologies, customer experiences, suppliers and third-party vendors?
- Do we deploy scenario analysis techniques to understand better how different scenarios will play out to recognise their implications to our strategy and business model? Are response plans updated for the insights gained from this process? Are action triggers and decision prompts put in place to offer early warning capability?
- Do we encourage the identification of opportunities to take on more risk on a managed basis? For example, is risk management effectively integrated with strategy-setting to help leaders make the best bets from a risk/reward standpoint that have the greatest potential for creating enterprise value?
- Are we monitoring the business environment over time for evidence of changes that may invalidate one or more critical assumptions underlying our organisation's strategy? If so, when there is evidence that one or more critical assumptions underlying the strategy are becoming, or have become, invalid, is this information along with actionable options presented to decision-makers on a timely basis? Does management act in a timely fashion on that knowledge to revisit the strategy and undertake necessary mid-course adjustments?
- Do the board and senior management receive risk-informed insights, competitive intelligence and information regarding opportunities to secure early-mover positioning in the marketplace?

Diagnostic theme: Assessing whether accountabilities for managing risks are clearly defined and supported

Following completion of a formal or informal risk assessment:

- Are risk owners assigned for newly identified risks? Are these owners held accountable for managing their assigned risks?
- Are effective risk response action plans developed to address the risk at the source? Are risk owners accountable for the design and execution of those responses?
- Is the organisation satisfied that its oversight and governance of its business continuity planning and operational resilience activities are sufficient in scope enterprisewide and not limited to certain aspects of the organisation (e.g., information technology, supply chain operations)?
- Is there an effort to source the root causes of certain risks that warrant an improved understanding of how they can be better managed? Does the sourcing process look for patterns that connect potential interrelated risk events?

- Do compensation and other incentive plans include explicit components related to the effectiveness of managing risks assigned to risk owners?
- Have we considered how our compensation and other incentive plans might unintentionally trigger significant risks, e.g., unwarranted risk taking?
- Do decision-making processes consider the impact of a particular decision on the organisation's risk profile?
  - Is there actionable, current risk information that is widely shared to enable more informed decision-making across the organisation?
  - Have we sufficiently communicated the relative value and importance of considering risk in decision-making across the enterprise?
  - Is the board sufficiently involved in the decision-making process, particularly when it involves a significant acquisition of a new business, entry into new markets, the introduction of innovative technologies or alteration of key assumptions underlying the strategy?
- Are significant risks related to the execution of the strategy and business model monitored over time to consider whether:
  - Changes or developments have occurred requiring corrective action?
  - The organisation continues to operate within established risk tolerances in meeting key business objectives?

Diagnostic theme: Assessing whether communications with the board provide an effective enterprise view of top risks that is insightful for board risk oversight

With respect to communicating and overseeing the risk profile:

- Is the board informed of the results of management's risk assessment on a timely basis? Do directors agree with management's determination of the significant risks?
- Are significant risk issues warranting attention by executive management and the board escalated to their attention on a timely basis? Does management apprise the board in a timely manner of significant emerging risks or significant changes in the organisation's risk profile?
- With respect to the most critical risks facing the organisation, do directors understand, at a high level, the organisation's responses to these risks? Is there an enterprisewide process in place that informs the board's risk oversight effectively, e.g., a risk dashboard?
- Is there a periodic board-level dialogue with management regarding the organisation's appetite for risk and whether the organisation's risk profile is aligned with that risk appetite?
- Is the board satisfied that the strategy-setting process appropriately considers a substantive assessment of the risks the enterprise is taking on as strategic alternatives are considered and the selected strategy is implemented?
- Do the insights, intelligence and information received from the risk management process foster more effective dialogue in the boardroom and C-suite regarding future opportunities, exposures and vulnerabilities?
- Given the organisation's risk profile, does the board periodically consider whether it has access to the diverse expertise and experience needed — either on the board itself or through access to external advisers — to provide the necessary oversight and advice to management? For example, is there sufficient digital savviness and experience on the board or in the boardroom?

Diagnostic theme: Assess the impact of leadership and culture on our risk management process

Because culture and leadership significantly impact the organisation's approach to risk oversight:

- Are the board's and C-suite's support for more robust risk management processes evident to key stakeholders across the organisation?
  - Is our risk management process helping to foster robust discussion and dialogue about the top risk issues among senior management and the board?
  - Is the board focused on advancing the organisation's risk management capabilities?
- Is there a willingness among the leadership team and business units to be more transparent about existing risk issues when sharing information with one another?
- Do we have an accurate read on how our organisation's culture is affecting the manner in which employees engage in risk management processes and conversations?
- Is our culture resilient enough to pivot in response to shifting customer preferences, changing employee expectations, new competitor actions, and unexpected developments in the supply chain and in third-party relationships?
- Are warning signs communicated by the risk management, compliance and ethics, or internal audit functions addressed in a timely fashion by executive and operational management?
- Do we have a "speak up" culture that encourages transparency and sharing of contrarian information and bad news? Are our employees convinced they can "speak up" without fear of repercussions to their careers or compensation? For example, does the process:
  - Encourage an open, positive dialogue for identifying and evaluating opportunities and risks?
  - Focus on reducing the risk of undue bias and groupthink?
  - Give adequate attention to differences in viewpoints existing across different executives and global jurisdictions?
- Is adequate attention given to red flags indicating warning signs of a dysfunctional culture that suppresses escalation of important risk information or encourages unacceptable risk taking?

These and other questions can assist organisations in defining their specific risks and assessing the adequacy of the processes informing their risk management and board risk oversight.

We hope the important insights about the perceived risks on the horizon for 2024 and a decade later (2034) provided in this report prove useful. We also hope that the insights, calls for action and the above diagnostic serve as a catalyst for an updated assessment of risks and improvements in risk management capabilities within organisations.

Research team and authors

NC State University's ERM Initiative

Mark Beasley
Professor and Director of the ERM Initiative

Bruce Branson
Professor and Associate Director of the ERM Initiative

Don Pagach
Professor and Director of Research of the ERM Initiative

Protiviti

Carol Beaumier
Senior Managing Director

Matthew Moore
Managing Director

Jim DeLoach
Managing Director

Kevin Donahue
Senior Director

Antonia Laplanche
Senior Manager

Shaun Lappi
Research Specialist

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, digital, legal, HR, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2023 *Fortune* 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of *Fortune* 100 and nearly 80 percent of *Fortune* 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

About NC State University's ERM Initiative

The Enterprise Risk Management (ERM) Initiative in the Poole College of Management at NC State University provides thought leadership about ERM practices and their integration with strategy and corporate governance. Faculty in the ERM Initiative frequently work with boards of directors and senior management teams helping them link ERM to strategy and governance, host executive workshops and educational training sessions, and issue research and thought papers on practical approaches to implementing more effective risk oversight techniques (www.erm.ncsu.edu).

protiviti®

NC STATE Poole College of Management
Enterprise Risk Management Initiative

www.protiviti.com

www.erm.ncsu.edu