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 | **Executive Summary**

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

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

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.

About the survey

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 was conducted in September and October of 2023 to capture perspectives on risks on the minds of executives as they peered into 2024. Each respondent was asked to rate 36 individual risk issues in terms of their 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 organisations a decade from now (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:

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**	

With regard to the respondents, 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 2034. Respondents to the survey serve in a number of different board and executive positions.

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[1] (OCS)	97
All Other[2]	87
Total number of respondents	**1,143**

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

[2] 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.

This executive summary provides a brief description of our methodology and an overview of the overall risk concerns for 2024 and 2034, as well as a review of the results by type of executive position and a series of calls to action. It concludes with diagnostic questions executives and directors may find helpful to consider when evaluating risk assessment and risk management processes.

In our full report (available online at erm.ncsu.edu or protiviti.com/toprisks), we analyse variances across different sizes and types of organisations, industry and respondent position, in addition to variations among organisations based in different geographic regions. Page 31 provides more details about our methodology. This executive summary highlights our key findings.

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).

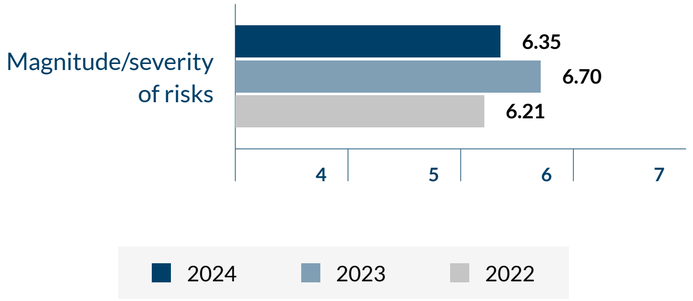
Risk levels declined from last year but remain higher than two years ago.

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	↓

TABLE 1

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	●	●	●	●	●	●	●	●	●	●

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.

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 executive summary 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.

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 2 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.

TABLE 2

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.

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