Executive Perspectives on Top Risks 2023 & 2032

Talent, culture, cybersecurity and data privacy represent top risk issues for public sector organisations

The level of uncertainty in today's global marketplace and the velocity of change continue to produce a multitude of potential risks that can disrupt an organisation's business model and strategy on very short notice. Unfolding events in Eastern Europe, changes in government leadership in several countries around the globe, escalating inflation, rising interest rates, ever-present cyber threats, competition for talent and specialised skill sets, continued disruptions in global supply chains, rapidly developing technologies … these represent just a sampling of the complex web of drivers of risks that may threaten an organisation's achievement of its objectives. Uncertainty and risk are here to stay. Keeping abreast of emerging risk issues and market opportunities is critical to improving organisational resilience.

The need for robust, strategic approaches to anticipating and managing risks cannot be overemphasised. Boards of directors and executive management teams who choose to manage risks on a reactive basis are likely to be left behind those who embrace the reality that risk and return are interconnected and recognise the benefits of proactively managing risks through a strategic lens. Those leaders who understand how insights about emerging risks can be used to navigate the world of uncertainty nimbly increase their organisation's ability to pivot when the unexpected occurs. That can translate into sustainable competitive advantage.

In this 11th annual survey, Protiviti and NC State University's ERM Initiative report on the top risks on the minds of global boards of directors and executives in 2023 and over the next 10 years, into 2032. Our respondent group, which includes 1,304 board members and C-suite executives from around the world, provided their perspectives about the potential impact over the next 12 months and next decade of 38 risk issues across these three dimensions:[1]

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

[1] Each respondent rated 38 individual risk issues using a 10-point scale, where a score of 1 reflects "No Impact at All" and a score of 10 reflects "Extensive Impact" to their organization. For each of the 38 risk issues, we computed the average score reported by all respondents.

Commentary – Public Sector Industry Group

In assessing the global risk landscape for public sector organisations in 2023 and 2032, familiar themes emerge: talent and the future of work, culture, cyber threats and data privacy.

The top risk issue in the public sector for 2023 is succession challenges and the ability to attract and retain top talent, while the second-ranked risk issue for these organisations is anticipated increases in the cost of labour. These are ongoing concerns for public sector organisations, as they compete with the private sector for talent and skills, particularly those required to drive innovation programs and technology transformation.

Interestingly, economic conditions potentially restricting growth opportunities are ranked in the top five risk issues for public sector organisations for 2023, even though federal, state and local public sector entities tend to be less affected by economic cycles. That said, the coming year appears to present potential challenges that public sector leaders do not see 10 years out, as economic conditions are not in the top 10 list of risks for this period.

Public sector leaders also expressed concerns about uncertainty in core supply chain ecosystems as well as organisational resilience and agility to manage an unexpected crisis. Because public sector agencies purchase large quantities of products and services, these understandably are significant issues. Supply chain and resilience challenges are of particular concern as they relate to IT and operational technology hardware and software.

Beyond these challenges, prevalent themes in the top risks for public sector organisations in the coming year as well as the next decade include cybersecurity, privacy and third-party risk. There are a number of important factors at play here that are driving these concerns. First, in the United States, the U.S. Government Accountability Office (GAO), in its latest cybersecurity guidance, notes that the federal government needs to elevate the nation's cybersecurity as the country faces grave and rapidly evolving threats.

Prevalent themes in the top risks for public sector organisations in the coming year as well as the next decade include cybersecurity, privacy and third-party risk.

Although the federal government has made some improvements, it needs to move with a greater sense of urgency commensurate with the rapidly evolving and grave threats to the country. Specific recommendations include the following:

- **Establish a comprehensive cybersecurity strategy and perform effective oversight**. In September 2018, the U.S. administration delivered a national cybersecurity strategy, followed by an implementation plan in June 2019 that details the executive branch's approach to managing the nation's cybersecurity. In September 2020, GAO reported that the national strategy and implementation plan addressed some, but not all, of the desirable characteristics of national strategies, such as goals and resources needed. The current administration needs to either update the existing strategy and plan or develop a new comprehensive strategy that addresses those characteristics. GAO also highlighted the need to define a central role for leading the implementation of the national strategy. In January 2021, the U.S. Congress established the Office of the National Cyber Director within the Executive Office of the President. Although establishing this position is an essential step forward, critical risks remain within supply chains, workforce management and emerging technologies. For example, in December 2020, GAO reported that none of the 23 U.S. government agencies in its review had fully implemented key foundational practices for managing information and communications technology supply chains.

Risk category	Top 10 2023 risk issues	Rating
Operational	Our organisation's succession challenges and ability to attract and retain top talent and labour amid the constraints of a tightening talent/labour market may limit our ability to achieve operational targets	6.46
Macroeconomic	Anticipated increases in labour costs may affect our ability to meet profitability targets	6.09
Macroeconomic	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	6.00
Strategic	Regulatory changes and scrutiny may heighten, noticeably affecting the way our processes are designed and our products or services are produced or delivered	5.98
Operational	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	5.96
Operational	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	5.95
Operational	Inability to utilise 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	5.78
Operational	Changes in the overall work environment including shifts to hybrid work environments, expansion of digital labour, 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	5.76
Operational	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 goals may prevent us from meeting organisational targets or impact our brand image	5.67
Operational	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	5.65

- **Secure federal systems and information**. The U.S. government has made some progress in securing systems. Nevertheless, federal agencies continue to have numerous cybersecurity weaknesses, due in large part to ineffective information security programs. Further, cyber incidents increasingly are posing a threat to government and private sector entities. The gravity of the threat was reinforced by the December 2020 discovery of a cyberattack that has had widespread impact on government agencies, critical infrastructure and the private sector. In 2019, GAO reported that most of the 16 agencies reviewed had incident response processes with key shortcomings, thereby limiting their ability to minimise damage from attacks.
- **Protect cyber critical infrastructure**. Critical infrastructure in the United States involves both public and private systems vital to national security. Since 2010, GAO has made nearly 80 recommendations to enhance infrastructure cybersecurity; for example, GAO recommended that agencies better measure the adoption of the National Institute of Standards and Technology (NIST) framework of voluntary cyber standards and correct sector-specific weaknesses. However, most of these recommendations (nearly 50) have not been implemented. As a result, the risks of unprotected infrastructures being harmed are heightened. Without question, this is a global challenge. In Australia, for example, the *Security of Critical Infrastructure Act 2018* requires owners and operators of critical infrastructure to take steps to safeguard vital assets. The Act subsequently was amended to broaden the scope of industry sectors, through a combination of *The Security Legislation Amendment (Critical Infrastructure) Act 2021* and *The Security Legislation Amendment (Critical Infrastructure Protection) Act 2022*. These two legislative reforms form the Commonwealth framework for critical infrastructure protection, as well as legislated last resort powers in the event of a catastrophic cyber security incident.
- **Protect privacy and sensitive data**. The U.S. federal government and private sector have struggled to protect privacy and sensitive data. Advances in technology have made it easy to collect information about individuals and ubiquitous internet connectivity has facilitated sophisticated tracking of individuals and their activities. The vast number of individuals affected by various data breaches has underscored concerns that personally identifiable information is not being protected adequately. GAO's reviews of agency practices to protect sensitive data have identified weaknesses and have resulted in numerous recommendations for agencies such as the U.S. Department of Housing and Urban Development, U.S. Department of Education and U.S. Internal Revenue Service.

Advances in technology have made it easy to collect information about individuals and ubiquitous internet connectivity has facilitated sophisticated tracking of individuals and their activities. The vast number of individuals affected by various data breaches has underscored concerns that personally identifiable information is not being protected adequately.

Risk category	Top 10 2032 risk issues	Rating
Operational	Our organisation's succession challenges and ability to attract and retain top talent and labour amid the constraints of a tightening talent/labour market may limit our ability to achieve operational targets	6.61
Strategic	Regulatory changes and scrutiny may heighten, noticeably affecting the way our processes are designed and our products or services are produced or delivered	6.54
Operational	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	6.50
Operational	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	6.25
Strategic	Rapid speed of disruptive innovations enabled by advanced technologies (e.g., artificial intelligence, 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 manage the risk appropriately, without making significant changes to our business model	6.17
Macroeconomic	The adoption of digital technologies (e.g., artificial intelligence, automation in all of its forms, natural language processing, visual recognition software, virtual reality simulations) in the marketplace and in our organisation may require new skills that either are in short supply in the market for talent or require significant efforts to upskill and reskill our existing employees	6.17
Operational	Inability to utilise 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	6.06
Strategic	Rapidly expanding developments in social media and platform technology innovations may significantly impact how we do business, interact with our customers, ensure regulatory compliance and/or manage our brand	6.02
Macroeconomic	Anticipated increases in labour costs may affect our ability to meet profitability targets	6.02
Operational	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	6.01

About the Executive Perspectives on Top Risks Survey

We surveyed 1,304 board members and executives across a number of industries and from around the globe, asking them to assess the impact of 38 unique risks on their organisation over the next 12 months and over the next decade. Our survey was conducted online in September and October 2022 to capture perspectives on the minds of executives as they peered into 2023 and 10 years out.

Respondents rated the impact of each risk on their organisation using a 10-point scale, where 1 reflects “No Impact at All” and 10 reflects “Extensive Impact.” For each of the 38 risks, we computed the average score reported by all respondents and rank-ordered the risks from highest to lowest impact.

Read our *Executive Perspectives on Top Risks Survey for 2023 and 2032* executive summary and full report at www.protiviti.com/toprisks or http://erm.ncsu.edu.

Contacts

Perry Keating
Managing Director
perry.keating@protiviti.com

Charles Dong
Managing Director
charles.dong@protiviti.com