The economy, cyber threats and talent drive concerns for government services leaders

by Charles Dong
Global Leader, Public Sector Practice, Protiviti

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.

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

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

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

Commentary – Government Services Industry Group

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

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

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

Overview of top risk issues in 2024

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

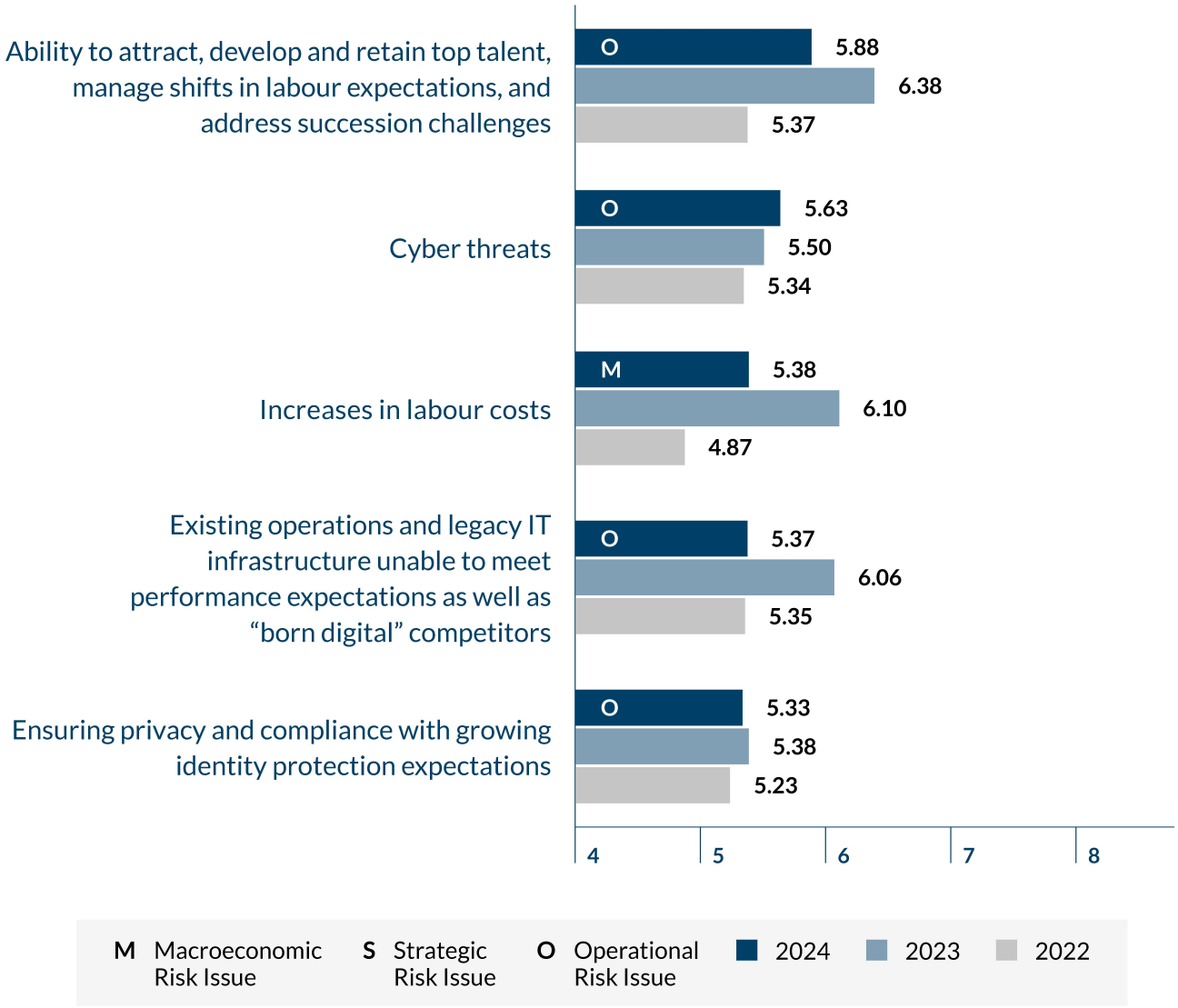
As leaders of government services organisations focus their attention on the most pressing and prevalent risks in 2024, they should consider new mindsets and approaches for managing talent, mitigating cyber threats and updating legacy IT infrastructure. Doing so requires a solid grasp of the multifaceted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

- **Talent management:** Attracting, recruiting and retaining skilled workers are ongoing — and borderline endemic — challenges within government services. These areas also represent a long-term problem: Survey respondents project talent-related risks as the second most significant concern in 2034, just behind cyber threats (see below). The historic allure of government service (e.g., situations such as the Cold War and Space Race, which provided strong, non-financial motivation) does not appear to be motivating younger workers to pursue government employment in the way people did in the latter half of the 20th century. Now, more "baby boom" engineers who leapt at the opportunity to work for space programs in the 1960s, 1970s and 1980s are retiring, and Gen X workers may not be far behind. From 2020 to 2022, an average of more than 100,000 U.S. federal workers retired each year. That's 36% higher compared to the period from 2000 to 2002, when approximately 76,000 federal workers retired annually.[2] Retirement-age federal employees now outnumber younger employees by two to one in the United States, where there were more full-time

[2] www.opm.gov/retirement-center/retirement-statistics/.

permanent federal employees in the 50—54 age bracket than any other age group in 2022.[3] Furthermore, across the globe, subsequent generations are far more likely to choose the allure and higher pay of jobs in industries such as technology and financial services over government roles. Of note, for 2024, other talent management-related concerns include increasing labour costs (the third highest-ranked risk issue) and the impact of social issues and DEI priorities on organisations' ability to attract and retain workers (a top 10 risk issue).

Government — 2024



- **Cybersecurity:** As is the case with talent management, cyber threats are an area of significant concern for government agencies. To illustrate, in the United States, over the past dozen years or so the U.S. Government Accountability Office (GAO) has publicly issued more than 700 recommendations related to securing federal systems and information. "Until these are fully implemented," a January 2023 GAO report states, "federal agencies will be more limited in their ability to protect private and sensitive data entrusted to

[3] https://usafacts.org/articles/how-old-is-the-federal-workforce/.

them."[4] Not surprisingly, ensuring privacy and compliance with growing identity protection expectations also ranks as a top 2024 risk issue among government services respondents. The same holds true for third-party risks (ranked in the top 10 for 2024), many of which relate directly to data privacy and security issues.

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

- **Legacy IT:** Government services organisations face scale, time, money and resource challenges when it comes to addressing aging IT infrastructures through technology modernisation. Mainframe systems designed in the 1970s and 1980s still underpin operations in many government offices. These infrastructures have been held together with numerous makeshift, ad hoc solutions by systems administrators who have already retired or will do so soon. In addition, given their age and design, many legacy systems have undergone extensive customisation. In many cases, this means that upgrades are off the table, and that new, modern systems must be implemented from scratch. While time-consuming and expensive, such implementations are crucial to perform because outdated systems can limit organisational resilience and agility (another top 10 risk concern for 2024) as well as the ability to recruit talented technology professionals who would rather work with advanced tools and technologies than perform troubleshooting and maintenance on antiquated systems. Additionally, more large ERP vendors are establishing definitive timelines for moving customers away from on-premises solutions to cloud environments, further underscoring the urgency to update legacy systems.

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

Overview of top risk issues in 2034

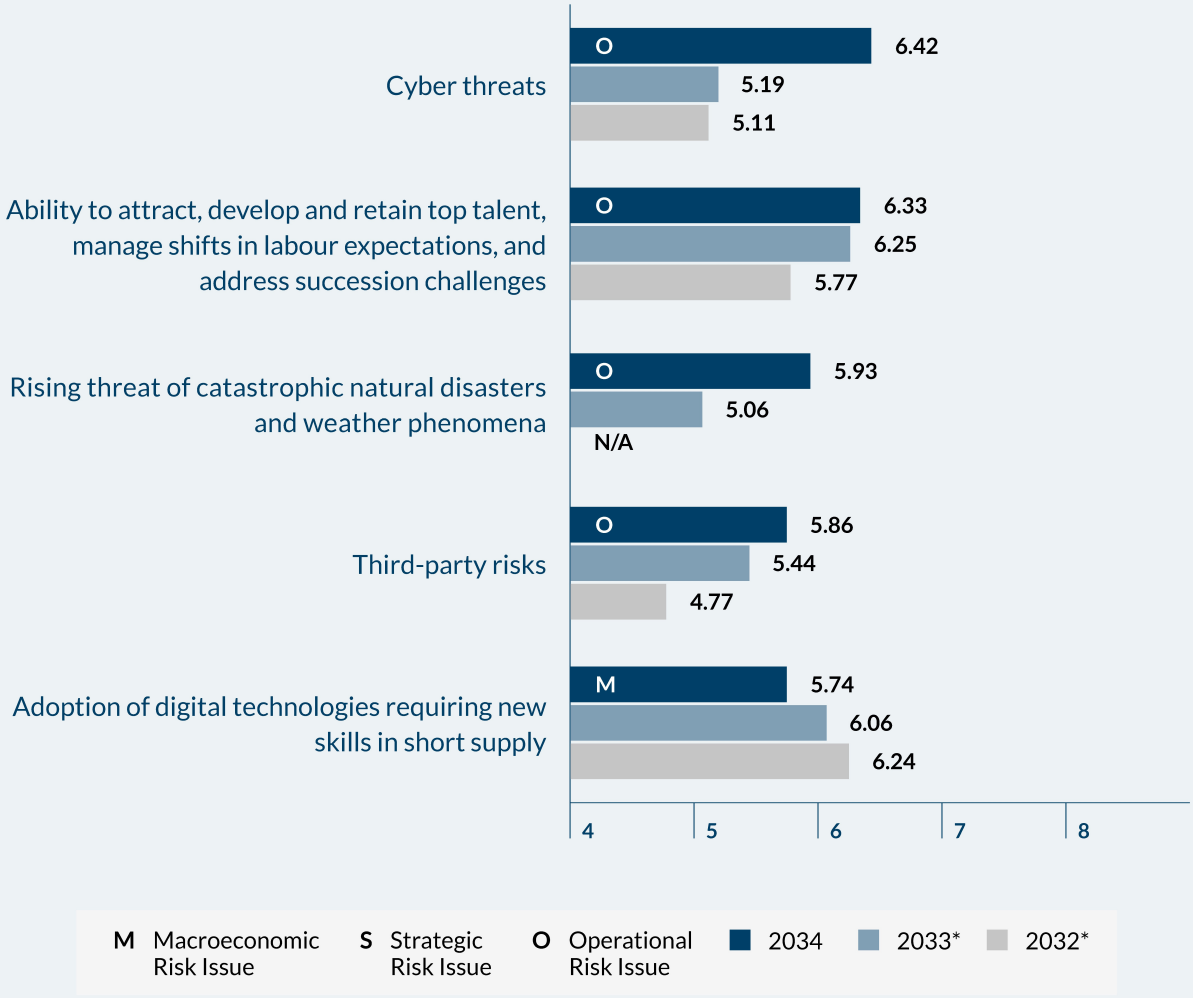
When government services leaders share their 10-year outlook, cybersecurity and talent management risk ratings are considerably higher, and they are joined by major concerns related to natural disasters and regulatory requirements focused on climate change and sustainability.

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

[4] www.gao.gov/products/gao-23-106428.

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

Government — 2034



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

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

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

About the Executive Perspectives on Top Risks Survey

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

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

Contact

Charles Dong
Managing Director, Public Sector Industry Leader
charles.dong@protiviti.com