Executive Perspectives on Top Risks 2023 & 2032

Talent, culture, cybersecurity and resiliency represent top risk issues for higher education institutions

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 organisation. For each of the 38 risk issues, we computed the average score reported by all respondents.

Commentary – Higher Education Industry Group

In assessing the global risk landscape for higher education organisations in 2023 and 2032, familiar themes emerge: talent and the future of work, culture, resiliency, data privacy and compliance, cyber threats, and more. The top-rated risk for the industry involves succession challenges and the ability to attract and retain top talent. Other highly rated risk issues include the organisation's approach to managing ongoing demands of remote and hybrid work environments, as well as concerns about adapting the business model to embrace the evolving "new normal" brought on by the pandemic and emerging social change.

Among the issues driving these concerns, there continues to be a high level of executive- and staff-level turnover within higher education institutions and open positions are proving to take longer and more difficult to fill. The industry already has to deal with a relatively small talent pool of candidates who have higher education industry experience. In addition, growing IT regulations continue to favour industry-agnostic frameworks and require professionals familiar with the latest requirements and technology trends to ensure compliance – skill sets that are particularly challenging to find within higher education.

Another contributor to the challenge is the need, or preference, for higher education staff to work on site versus having the advantages of a hybrid or remote work model. Given persistently low unemployment levels and the resulting options job candidates have, it's understandable to find many higher education institutions struggling to attract and retain people. There may be a need for a change in mindset and culture (see below) to improve long-term employee and student engagement.

Given persistently low unemployment levels and the resulting options job candidates have, it's understandable to find many higher education institutions struggling to attract and retain people.

In regard to the higher education business model, factors at play include increases in online or hybrid environments in higher education, together with greater demands among students and staff to employ these approaches; ongoing discussion and debate about the cost and debt associated with obtaining a degree; and the potential impact of offering micro credentials.

Two other highly rated risks for higher education institutions relate to culture and resilience – specifically, that the organisation's culture may not encourage the timely identification and escalation of risk issues and market opportunities, and that the organisation may not be sufficiently resilient and/or agile to manage an unexpected crisis. These concerns are understandable. Decentralised federated IT models continue to prevent higher education organisations from leveraging employee skill sets across colleges and lead to a lack of consistency and maturity across the enterprise. Further, aging technology infrastructure and a heavy dependence on traditional on-premise environments combined with the higher education industry's reality of generally lower budgets for modernisation raises the impact of these types of events when they are technology-related.

More higher education institutions are focusing on formalising and maturing their enterprise risk management functions, which places a brighter spotlight on culture and resiliency. In addition, most higher education institutions operate in a decentralised model, which tends to exacerbate culture- and resilience-related issues.

Another related area of concern is third-party risk management – there may be a lack of understanding about risk exposures resulting from third-party operations that are not fully aligned with an institution with regard to potential risk issues as well as market opportunities. Finally, ongoing concerns among higher education institutions

regarding security and fraud risk likely are focusing greater attention among members of the board and C-suite on culture and resiliency.

In fact, ensuring data privacy and compliance with growing identity protection expectations and regulations ranks among the top risk issues for higher education institutions, as does the risk that the organisation may not be sufficiently prepared to manage cyber threats such as ransomware.

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	6.17
Operational	Our organisation's culture may not sufficiently encourage the timely identification and escalation of risk issues and market opportunities that have the potential to significantly affect our core operations and achievement of strategic objectives	6.00
Strategic	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	5.83
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	5.83
Operational	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 may negatively impact our ability to retain talent as well as the effectiveness and efficiency of how we operate our business	5.78
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	5.61
Macroeconomic	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	5.59
Strategic	Our organisation may not be able to adapt its business model to embrace the evolving "new normal" imposed on our business by the ongoing pandemic and emerging social change	5.44
Operational	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	5.44
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	5.39

Risk of cyber attacks remains a critical concern for these organisations given that, due to perceived security weaknesses along with a lack of security awareness among students and staff, they remain a prime target for cyber and ransomware attacks. Data breach response readiness is critical considering it is a matter of when, not if, student and employee data is lost, stolen or compromised. In addition, the number of data- and privacy-related regulations – at the federal, state and local levels – that are applicable to higher education institutions continues to grow. Many are not leveraging industry-leading tools to improve their security posture and, as detailed above, are struggling to attract and retain qualified IT talent. Further, many of these organisations increasingly are centralising their IT functions through use of the cloud and other technology initiatives but they have not centralised risk management.

Diversity, equity and inclusion issues – specifically, shifts in perspectives and expectations about social issues and priorities surrounding DEI – rank as high-risk priorities, as well. Significant progress has been achieved in equality, particularly gender, which is important given that student bodies continue to demand changes and greater representation. However, many of these initiatives tend to be undertaken in silos within higher education institutions and can become disjointed. Boards and executive management should look for opportunities to organise and centralise these initiatives to achieve greater synergy and consistency.

Regarding the long-term risk outlook for higher education, board members and C-suite leaders looking out to 2032 see similar concerns for their organisations – among them, talent, culture, cyber threats and resiliency. Data privacy and compliance with identity protection expectations and regulations is the top risk for the 2032 time horizon, while cyber threat preparedness ranks third.

A notable addition to the top 10 risks for 2032 is the concern that existing operating processes, talent, legacy IT infrastructure, lack of digital expertise and/or insufficient digital knowledge in the C-suite and boardroom may result in failure to meet performance expectations, especially when compared with organisations that are “born digital” or investing heavily to leverage technology. This is a strong indicator that while innovation, transformation and the adoption of digital technologies may not be as much of a near-term concern for boards and C-suite leadership within higher education institutions, they do represent a significant concern over the next decade from the standpoint of ensuring the long-term success of their organisations.

Calls to action for higher education leaders

- Make succession planning a strategic priority; prioritise and integrate upskilling and retention strategies, and ensure the organisation is offering competitive compensation.
- Build a resilient culture; consider opportunities to implement more flexible scheduling throughout the organisation.
- Evaluate non-higher education organisational models for running the operation and adopt common processes across institutions.
- Consider non-traditional staffing models, including nonlocal resources, contract professionals, etc.
- Establish an ERM program with appropriate board-level oversight.
- Establish a comprehensive third-party risk management program to ensure compliance with regulations and best practices and to understand the organisation’s risk exposures.
- Organise IT risk functions consistent with other risk management functions in the institution.

- Identify all applicable IT-related regulations and establish a controls framework to govern the IT organisation – frameworks can be flexible but should be based fully or partially on industry-recognised standards such as NIST.
- Focus, and adjust as needed, the institution's business model to align with its core programmatic competencies to enhance the educational quality and value offered to students.

Risk category	Top 10 2032 risk issues	Rating
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	6.44
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	6.28
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	6.28
Operational	Our organisation's culture may not sufficiently encourage the timely identification and escalation of risk issues and market opportunities that have the potential to significantly affect our core operations and achievement of strategic objectives	5.78
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	5.78
Operational	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 may negatively impact our ability to retain talent as well as the effectiveness and efficiency of how we operate our business	5.78
Operational	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	5.67
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	5.67
Strategic	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	5.61
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	5.61

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

Eric Groen
Managing Director
eric.groen@protiviti.com

Charles Dong
Managing Director
charles.dong@protiviti.com

Tonya Baez
Director
tonya.baez@protiviti.com