JOURNAL OF POLITICAL SCIENCE, LAW & GOVERNANCE

EMERGENCE OF GLOBAL RISKS SINCE 2000 AND THE RELUCTANCE OF ORGANIZATIONS TO FULLY EMBRACE RISK MANAGEMENT PRACTICES

DR SONJAI KUMAR, CFIRM, SIRM

Certified Fellow of the Institute of Risk Management, London

Corresponding Author: DR SONJAI KUMAR

Abstract

The emergence of global risks since the year 2000 has reshaped the dynamics of organizational resilience, governance, and strategy. This paper examines the trajectory of systemic risks—including financial crises, terrorism, pandemics, climate change, cyber threats, and geopolitical instability—while highlighting organizational responses and the persistent reluctance to adopt comprehensive risk management frameworks. Beginning with the dot-com collapse and the September 11 terrorist attacks, the early twenty-first century demonstrated the fragility of interconnected global systems. Subsequent crises, such as the 2007–2008 financial collapse, the intensification of climate-related events, and the COVID-19 pandemic, further revealed structural deficiencies in risk preparedness and response mechanisms. Cybersecurity incidents and the ethical challenges posed by emerging technologies such as artificial intelligence have underscored the risks' dynamic and multidimensional nature in an increasingly digitalized world.

Despite recurring crises, organizational adoption of robust risk management practices remains inconsistent. Key factors contributing to this reluctance include short-termism, resource constraints, regulatory gaps, organizational culture, and cognitive biases that underestimate risk exposure. These barriers perpetuate vulnerabilities and hinder the institutionalization of proactive risk governance. The consequences of neglecting risk management are significant, encompassing financial instability, reputational erosion, operational fragility, and strategic obsolescence.

This article argues for the urgent integration of risk management into organizational strategy, governance, and culture. Recommendations include board-level engagement, cross-functional collaboration, scenario analysis, technological integration, and proactive stakeholder communication. By transitioning from a reactive to a proactive paradigm, organizations can convert risk management into a source of competitive advantage and long-term sustainability. Ultimately, risk management should not be regarded merely as a compliance exercise but as a strategic imperative central to organizational resilience in an era defined by volatility, uncertainty, complexity, and ambiguity (VUCA).

INTRODUCTION

The onset of the twenty-first century has been marked by intensified globalization, rapid technological progress, and heightened interdependencies among nations, organizations, and individuals. While these developments have created unprecedented opportunities, they have simultaneously generated complex, multifaceted, and often systemic risks. Financial crises, geopolitical instability, pandemics, climate change, and cyber threats have demonstrated the fragility of interconnected systems and underscored the need for robust risk governance. Yet, despite the proliferation of such events, empirical evidence suggests that many organizations remain hesitant to adopt comprehensive risk management practices. This paper examines the emergence of global risks since 2000, provides illustrative examples, and explores underlying reasons for organizational reluctance to integrate risk management into their strategic and operational frameworks.

JOURNAL OF POLITICAL SCIENCE, LAW & GOVERNANCE

THE EVOLUTION OF GLOBAL RISKS SINCE 2000

1. THE DOT-COM BUBBLE (2000–2002)

The collapse of overvalued technology enterprises at the beginning of the twenty-first century revealed deficiencies in investor due diligence and highlighted systemic vulnerabilities within financial markets (Shiller, 2000). The bubble burst emphasized the necessity of robust risk evaluation methods in investment and corporate strategies.

2. SEPTEMBER 11 ATTACKS (2001)

The terrorist attacks of September 11, 2001, constituted a significant geopolitical shock with far-reaching consequences for global aviation, insurance, and security infrastructures. In addition to the tragic human loss, the event precipitated increased regulatory scrutiny, enhanced counterterrorism measures, and elevated awareness of security-related risks (Enders & Sandler, 2012).

3. THE GLOBAL FINANCIAL CRISIS (2007–2008)

Originating in the subprime mortgage market in the United States, the global financial crisis demonstrated the fragility of interconnected banking and financial systems. It exposed weaknesses in governance, risk oversight, and regulatory compliance. The subsequent economic downturn, institutional bailouts, and loss of public trust underscored the systemic importance of financial risk management (Acharya & Richardson, 2009).

4. CLIMATE CHANGE AND ENVIRONMENTAL RISKS

The increasing frequency and severity of climate-related disasters, including Hurricane Katrina (2005), the Australian bushfires (2019–2020), and recurrent flooding events, have reinforced the urgency of incorporating environmental and climate risks into corporate risk frameworks. Scientific consensus confirms that climate change constitutes a critical and long-term threat to organizational resilience (IPCC, 2021).

5. CYBERSECURITY THREATS

With the expansion of digitalization, organizations have been exposed to escalating risks of cyberattacks. Breaches such as the Target data breach (2013), the WannaCry ransomware attack (2017), and the SolarWinds incident (2020) highlight the vulnerabilities inherent in digital infrastructure and the need for comprehensive cybersecurity risk management (Anderson et al., 2019).

6. COVID-19 PANDEMIC (2020–2022)

The COVID-19 pandemic represents a defining systemic risk of the twenty-first century. Its global ramifications encompassed disruptions to supply chains, workforce transitions to remote environments, macroeconomic downturns, and strains on healthcare systems. The pandemic revealed widespread deficiencies in preparedness and emphasized the necessity of scenario-based risk management (Nicola et al., 2020).

7. GEOPOLITICAL CONFLICTS AND TRADE WARS

The escalation of geopolitical tensions, notably the Russia-Ukraine conflict (2014, 2022) and trade frictions between the United States and China, has disrupted energy markets, trade flows, and global supply chains. These events illustrate the increasing salience of political risk in global business operations (Kobrin, 2020).

8. TECHNOLOGICAL AND ARTIFICIAL INTELLIGENCE RISKS

The proliferation of artificial intelligence, automation, and big data analytics has introduced new risks, including algorithmic bias, ethical concerns, job displacement, and privacy violations. These risks highlight the need for organizations to balance innovation with ethical and operational safeguards (Floridi & Cowls, 2019).

EXPLAINING ORGANIZATIONAL RELUCTANCE TO EMBRACE RISK MANAGEMENT

Despite repeated demonstrations of the significance of global risks, organizational adoption of comprehensive risk management remains inconsistent. Several factors contribute to this reluctance:

1. **Short-Termism:** Organizations frequently prioritize short-term profitability and shareholder value over long-term resilience. Risk management investments are often perceived as costs rather than as mechanisms for safeguarding sustainable growth (Porter, 1992).

2. **Perceived Complexity of Risk Frameworks:** Frameworks such as Enterprise Risk Management (ERM) necessitate structural adjustments, cultural shifts, and resource allocation. Many organizations perceive these requirements as administratively burdensome (Fraser & Simkins, 2010).

3. **Cognitive Bias and Risk Underestimation:** Leaders may succumb to optimism bias, assuming that adverse events are improbable within their own organizations. This cognitive distortion fosters complacency (Kahneman, 2011).

4. **Regulatory Gaps:** In sectors and jurisdictions with limited regulatory enforcement, the absence of external compulsion diminishes the perceived necessity for rigorous risk management (Power, 2004).

5. **Organizational Culture:** Risk management is confined to compliance or audit functions in numerous organisations rather than embedded into strategic planning. This siloed approach diminishes effectiveness and integration (Schein, 2010).

6. **Resource Constraints:** Small and medium enterprises (SMEs) may perceive the financial and human resource costs associated with risk management frameworks as prohibitive (Beasley et al., 2005).

7. **Uncertainty in Risk Quantification:** Emerging risks such as climate change, cyber threats, and pandemics are inherently challenging to model quantitatively, leading to delays in adoption due to uncertainty (Taleb, 2007).

CONSEQUENCES OF INADEQUATE RISK MANAGEMENT

The failure to institutionalize risk management produces multiple adverse outcomes: - Financial Vulnerability: As exemplified by the 2008 financial crisis, inadequate risk oversight can precipitate systemic institutional failures. - Reputational Damage: Data breaches and compliance failures erode stakeholder trust. - Operational Fragility: The COVID-19 pandemic highlighted weaknesses in global supply chains and workforce preparedness. - Regulatory Exposure: Non-compliance with statutory frameworks results in penalties, litigation, and reputational harm. - Strategic Obsolescence: Inability to adapt to technological and environmental transitions may lead to long-term irrelevance.

TOWARDS A RISK-RESILIENT FUTURE

Addressing these deficiencies requires organizations to institutionalize risk management as a core component of strategic governance. Key recommendations include:

1. **Integration of Risk into Strategy:** Risk management should be embedded within corporate strategy, capital allocation, and innovation frameworks.

2. **Board-Level Engagement:** Effective risk governance necessitates active oversight and sponsorship by boards of directors.

3. **Leveraging Technological Tools:** Predictive analytics, artificial intelligence, and big data can enhance foresight and early warning systems.

4. **Cross-Functional Collaboration:** Risk management must transcend functional silos, incorporating insights from finance, operations, IT, HR, and compliance.

5. **Capacity Building:** Continuous training and awareness initiatives should empower employees to identify and mitigate risks at all levels.

6. **Scenario Analysis and Stress Testing:** Organizations should employ scenario modeling to prepare for extreme but plausible disruptions.

7. **Transparency and Stakeholder Engagement:** Proactive disclosure of risk exposures and mitigation strategies builds trust and resilience.

CONCLUSION

Since 2000, global risks have proliferated in scale, scope, and interconnection. Financial crises, terrorism, pandemics, climate change, cyber threats, and geopolitical tensions illustrate the complex and systemic nature of risks in a globalized era. Nonetheless, organizational adoption of risk management practices has lagged due to short-termism, cultural barriers, regulatory gaps, and resource limitations. The consequences of inaction include financial instability, reputational harm, operational fragility, and strategic obsolescence.

Organizations must transition from reactive to proactive risk management to navigate an increasingly uncertain environment. Embedding risk resilience within organizational DNA will not only mitigate vulnerabilities but also create competitive advantage. In this context, risk management must be regarded not as a compliance exercise but as a strategic imperative central to organizational sustainability.

REFERENCES

1. Acharya, V. V., & Richardson, M. (2009). Restoring financial stability: How to repair a failed system. Wiley.
2. Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M., Levi, M., … & Savage, S. (2019). Measuring the cost of cybercrime. Journal of Cybersecurity.
3. Beasley, M., Clune, R., & Hermanson, D. R. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. Journal of Accounting and Public Policy.
4. Enders, W., & Sandler, T. (2012). The political economy of terrorism. Cambridge University Press.
5. Floridi, L., & Cowls, J. (2019). A unified framework of five principles for AI in society. Harvard Data Science Review.
6. Fraser, J., & Simkins, B. J. (2010). Enterprise risk management: Today's leading research and best practices. Wiley.
7. IPCC. (2021). Climate Change 2021: The Physical Science Basis. Cambridge University Press.
8. Kahneman, D. (2011). Thinking, fast and slow. Farrar, Straus and Giroux.
9. Kobrin, S. J. (2020). Global political risk: Changing dimensions of risk in the twenty-first century. Thunderbird International Business Review.
10. Nicola, M., Alsafi, Z., Sohrabi, C., Kerwan, A., Al-Jabir, A., Iosifidis, C., … & Agha, R. (2020). The socio-economic implications of the coronavirus pandemic. International Journal of Surgery.
11. Porter, M. E. (1992). Capital disadvantage: America's failing capital investment system. Harvard Business Review.
12. Power, M. (2004). The risk management of everything: Rethinking the politics of uncertainty. Demos.
13. Schein, E. H. (2010). Organizational culture and leadership. Jossey-Bass.
14. Shiller, R. J. (2000). Irrational exuberance. Princeton University Press.
15. Taleb, N. N. (2007). The Black Swan: The impact of the highly improbable. Random House.