



The Next Generation of Business Risk Emerging Threats and the Growing Complexity of Corporate Vulnerability

Nurul Najiha Abdulloh^{1*}, Shahri Abu Seman², Zila Zainal Abidin³

¹ Faculty of Business and Accountancy, Universiti Poly-Tech Malaysia, Malaysia

^{2,3} Institute of Graduate Studies, Universiti Poly-Tech Malaysia, Malaysia

CORRESPONDING AUTHOR

Nurul Najiha Abdulloh
Email: nurul_najiha@uptm.edu.my
ORCID: 0000-0000-0000-0000

ARTICLE HISTORY

Received	Revised	Accepted	Published
29 June 2026	8 August 2026	2 September 2026	30 September 2026

ABSTRACT

Business risk is entering a fundamentally different era in which corporate vulnerability is shaped less by the presence of individual threats than by the speed, connectivity, and intensity through which disruptions interact across organisational systems. This article critically examines the changing architecture of business risk by exploring the convergence of geopolitical instability, artificial intelligence, cyber exposure, climate disruption, financial pressure, and increasingly fragile supply networks. Rather than viewing these threats as independent categories, the analysis demonstrates how contemporary vulnerabilities can migrate across functional and organisational boundaries, transforming an external disturbance into interconnected operational, financial, technological, strategic, and reputational consequences. Particular attention is given to the paradoxical role of technology, which strengthens predictive capability and organisational responsiveness while simultaneously creating new dependencies, cyber vulnerabilities, and failure pathways. The article further establishes organisational resilience as a strategic capability that extends beyond recovery towards adaptation and structural transformation under increasingly unpredictable conditions. It proposes a forward looking risk management orientation centred on integrated enterprise risk intelligence, geopolitical and supply network diversification, stronger digital and cyber governance, climate informed decision making, and transformative resilience. The article concludes that future corporate resilience will depend not simply on an organisation's ability to identify emerging threats, but on its capacity to understand how vulnerabilities propagate, reinforce one another, and reshape strategic exposure across the wider business ecosystem.

Keywords: Vulnerability, Resilience, Geopolitics, Cybersecurity, Adaptability

HOW TO CITE

Author1, A. A., & Author2, B. B. (20XX). Title of the article.
International Journal of Business and Management Advancement,
X(X), xx–xx. <https://doi.org/10.1000/ijbma.10000>

COPYRIGHT & OPEN ACCESS

Copyright © 2026 The Author(s).
Published by Global Academia Network. This open access article is
licensed under the Creative Commons Attribution (CC BY 4.0)
licence: <https://creativecommons.org/licenses/by/4.0/legalcode>

1. INTRODUCTION

Corporate vulnerability is no longer shaped by isolated threats that can be identified, quantified, and controlled through conventional risk management routines. A more intricate risk environment has emerged in which geopolitical instability, cyber exposure, technological dependence, climate disruption, supply chain fragility, financial volatility, and regulatory uncertainty can develop simultaneously and transmit consequences across organisational boundaries. Recent evidence demonstrates the interconnected character of these exposures. Liu et al., (2025) find that misalignment in firms' perceptions of political risk can significantly weaken operational resilience, particularly through supply chain network relationships. Abdelhedi and Ben Hamida (2026) similarly demonstrate persistent relationships among geopolitical risk, supply chain pressure, and the volatility of major firms, indicating that external disturbances can propagate into corporate performance through multiple channels. From a broader resilience perspective, Hosseini Shekarabi et al., (2025) identify disruption mitigation, robust optimisation, technological solutions, and adaptive capabilities as increasingly important components of contemporary supply chain resilience. These developments suggest that the next generation of business risk cannot be understood simply by extending traditional risk categories. The underlying architecture of corporate vulnerability itself is changing as firms become more digitally connected, internationally interdependent, environmentally exposed, and operationally reliant on networks whose behaviour extends beyond direct managerial control. This interpretation is consistent with Anton and Nucu (2020), who connect organisational uncertainty with risk perception and managerial judgement. This broader perspective improves strategic awareness.

Geopolitical instability represents one of the clearest examples of how contemporary risks can migrate from the external environment into the internal economics of a firm. Political conflict, trade restrictions, diplomatic tensions, sanctions, resource competition, and changes in international relations can alter sourcing conditions, transportation routes, market access, investment confidence, and operating costs with limited warning. Empirical evidence increasingly demonstrates that these consequences extend considerably beyond temporary market uncertainty. Research published in *Economics Letters* finds that geopolitical crises significantly increase supply chain risk through the erosion of resilience, greater customer concentration, and deterioration in inventory liquidity. Liu et al., (2025) further establish that inaccurate alignment between perceived political risk and supply chain partners can reduce operational resilience, illustrating that vulnerability depends not only on the existence of external threats but also on how effectively organisations interpret them. Dong et al., (2025) provide additional evidence that geopolitical risk negatively affects supply chain resilience, although artificial intelligence can strengthen resilience under particular industrial conditions. Such findings reveal an important transformation in business risk. External geopolitical events can rapidly become operational, financial, inventory, supplier, and strategic problems. Risk categories that were traditionally managed independently are consequently becoming increasingly interconnected, requiring firms to evaluate not only individual threats but also the pathways through which one disruption can amplify another. This requires decision makers to examine dependencies, concentration points, response capacity, and the speed at which disruption can move between functions and external partners.

Digital transformation introduces an equally significant paradox because technologies developed to strengthen productivity and decision quality can simultaneously generate new forms of corporate

exposure. Artificial intelligence, cloud infrastructure, interconnected production systems, digital platforms, and extensive data networks have expanded organisational capabilities while increasing dependence on complex technological ecosystems. Latsiou and Lambrinoudakis (2026) demonstrate that cyber supply chain risk requires organisations to move beyond isolated information security controls towards systematic identification, assessment, and treatment of vulnerabilities distributed throughout interconnected supply networks. The risk implications of artificial intelligence are similarly multidimensional. McLemore and Mihov (2026), using supervisory data from large United States bank holding companies, find that greater AI investment is associated with higher operational losses, particularly through external fraud, client related problems, and system failures, with stronger effects among organisations possessing weaker risk management practices. At the same time, AI can strengthen organisational responses to uncertainty. Research published in 2026 demonstrates that AI can improve managerial responsiveness and decision precision under fluctuating risk conditions, although it may also reduce managers' perceptions of risk. Technology therefore occupies a dual position within the emerging risk landscape. It can operate simultaneously as a mechanism for detecting and mitigating threats and as a source of new operational, governance, cybersecurity, and decision vulnerabilities. The need to balance technological capability with responsible organisational control is similarly emphasised by Orwat et al., (2024).

Environmental exposure further expands the boundaries of corporate risk by transforming climate change from a predominantly sustainability concern into a material financial and strategic consideration. Physical hazards can disrupt production facilities, transportation infrastructure, energy systems, agricultural inputs, labour availability, and supplier operations, while transition pressures can alter regulation, capital requirements, technology investment, customer preferences, and competitive positioning. Naseer et al., (2025), drawing on international evidence, find that corporate climate risk exposure increases market volatility, while stronger corporate governance and research and development intensity can moderate these effects. Research covering 2,146 nonfinancial firms across 34 countries similarly demonstrates a significant relationship between climate change risk and corporate risk taking, while board gender diversity and environmental, social, and governance performance influence this relationship. The significance of these findings lies in the movement of climate exposure across traditional organisational boundaries. An environmental event can become a production interruption, logistics failure, commodity price shock, insurance burden, financing constraint, reputational challenge, or strategic investment problem. Corporate vulnerability consequently emerges from combinations of exposures rather than from environmental risk operating independently. Modern risk management must therefore recognise that the financial consequences of climate disruption are increasingly transmitted through operational systems, markets, supply networks, governance structures, and long-term strategic decisions. Such an approach strengthens visibility of secondary consequences that may otherwise remain hidden until a local disturbance has already become an enterprise-wide problem.

The defining feature of the emerging business risk landscape is consequently not the existence of more risks, but the increasing complexity of their interaction, transmission, and amplification. A geopolitical shock can interrupt supply networks, generate commodity volatility, intensify financial pressure, and require strategic restructuring. A cyber incident can simultaneously compromise data, suspend production, damage customer confidence, interrupt suppliers, and create regulatory exposure. Climate disruption can affect infrastructure, inventory, insurance, financing, and market

demand, while technological solutions introduced to manage these problems may generate additional operational dependencies. Contemporary supply chain research reflects this shift towards multidimensional risk management. Hosseini Shekarabi et al., (2025) emphasise the integration of mitigation, robustness, technology, and resilience in addressing increasingly complex disruptions. Abudu et al., (2025), through a meta-analysis involving 52 empirical studies and 22,955 observations, further distinguish adaptive resilience from transformative resilience, indicating that organisations require both recovery capabilities and longer term structural adaptation to navigate major disruptions. Research on supply chain risk management capabilities similarly identifies warning, robustness, and resilience as distinct but interconnected capabilities required for contemporary disruption management. Against this background, this article examines the next generation of business risk by exploring how emerging threats are reshaping corporate vulnerability and why organisations must progress from fragmented risk control towards integrated, anticipatory, and adaptive approaches capable of protecting resilience in an increasingly interconnected business environment.

2. LITERATURE REVIEW

Research on business risk has progressively moved beyond the assumption that organisations confront independent categories of exposure that can be managed through specialised functional controls. Contemporary scholarship instead portrays vulnerability as an outcome of interacting technological, geopolitical, operational, financial, environmental, and network dependencies whose effects can travel rapidly across organisational boundaries. Monazzam and Crawford (2024) demonstrate that enterprise risk management contributes to organisational resilience through risk governance, risk culture, risk awareness, and the continuous alignment of risk practices with corporate strategy. Hosseini Shekarabi et al., (2025) extend this perspective within supply chain research by identifying optimisation, technology adoption, disruption management, and resilience strategies as interconnected research domains rather than isolated managerial concerns.

2.1 Enterprise Risk Evolution Reshaping Contemporary Corporate Vulnerability

Conventional risk management developed largely around the identification and treatment of recognisable categories such as financial, operational, legal, market, and strategic risk. This functional separation provided managerial clarity, but it becomes less effective where several exposures interact and generate consequences beyond the organisational unit responsible for the original threat. Anton and Nucu (2020) position enterprise risk management as an integrated approach intended to overcome fragmented risk practices by connecting risk identification and treatment across the organisation. More recent evidence reinforces the importance of this integration. Monazzam and Crawford (2024) find that risk governance frameworks, organisational culture, risk artefacts, and risk awareness contribute to resilience capabilities and that the evolution from traditional risk management towards enterprise risk management is an ongoing process rather than a completed organisational transition. Gleißner and Berger (2024) similarly argue for decision-oriented enterprise risk management that connects risk aggregation, value drivers, organisational processes, and strategic decision making instead of concentrating narrowly on risk minimisation. These perspectives demonstrate an important conceptual development. Risk management is increasingly expected to explain how combinations of uncertainty affect strategic objectives and organisational value. Corporate vulnerability therefore reflects not only the magnitude of individual threats, but also weaknesses in the organisation's capacity to recognise relationships among

exposures before they accumulate into material disruption. Operational interdependence is also evident in Monazzam and Crawford (2024), where strategic warehouse management is linked to supply chain performance under changing business conditions.

Broader resilience scholarship provides further support for understanding vulnerability as a dynamic organisational condition. Dahmen (2023) argues that organisational resilience should be regarded as an important property of enterprise risk management in responding to novel and severe crises, particularly because contemporary environments are characterised by complexity and multilinear relationships among risks. Paul and Saha (2025) similarly demonstrate that resilience has become integral to managing supply chain risk and disruption, with flexible strategies playing an important role in maintaining performance under adverse conditions. Hosseini Shekarabi et al., (2025), based on 294 peer-reviewed articles extracted from Web of Science and Scopus, identify risk mitigation, robust optimisation, technological solutions, and resilience strategies as central components of the evolving resilience literature. This development changes the intellectual emphasis from protecting organisations against predefined threats towards building capabilities that allow firms to continue functioning under conditions that cannot be completely anticipated. Corporate vulnerability should consequently be understood as the product of exposure combined with insufficient adaptive capacity. An organisation may possess sophisticated controls for individual risks yet remain vulnerable if those controls cannot recognise cascading consequences, coordinate responses across functions, or adapt when the character of disruption differs substantially from previous experience. Organisations that integrate these considerations into routine planning are better positioned to recognise weak signals before they develop into mutually reinforcing operational and financial pressures.

2.2 Geopolitical Exposure Intensifying Global Business Network Fragility

Political uncertainty has become increasingly embedded within operational risk because modern firms depend extensively on cross-border suppliers, logistics corridors, customers, financial systems, and institutional relationships. Geopolitical events can therefore generate consequences far beyond the countries directly involved in political confrontation. Chang et al., (2025) provide international evidence that geopolitical risk significantly weakens global supply chain resilience, with reduced trade credit and increased inventory costs operating as important transmission channels. Liu et al., (2025) extend this understanding by examining perceived political risk misalignment between buyers and suppliers. Their analysis of 1,421 supplier buyer dyads shows that misalignment in political risk perceptions significantly reduces operational resilience, while supply network structure influences the strength of this relationship. These findings are important because they demonstrate that vulnerability is generated not merely by geopolitical events themselves, but also by differences in how interconnected organisations recognise and respond to those events. A firm may therefore be strategically prepared for a political disruption while remaining exposed because critical suppliers, customers, or network partners interpret the same threat differently and adopt incompatible responses. This systems perspective also discourages excessive confidence in a single control because the effectiveness of any safeguard depends on the wider network in which it operates. For managers, the practical implication is that exposure must be assessed through transmission pathways rather than through a static register of isolated risk categories.

Recent research further reveals that geopolitical risk creates cascading effects across several traditional risk categories. López et al., (2025), through a systematic review of 80 studies, identify

six forms of geopolitical supply chain disruption and demonstrate that their management requires combinations of financial management, collaboration, resilience, and viable supply chain strategies. Chang et al., (2025) show that geopolitical exposure can weaken resilience through financial and inventory mechanisms, illustrating how political uncertainty can migrate into working capital, operational continuity, and supply availability. Additional empirical evidence indicates that geopolitical crises increase supply chain risk through resilience erosion, greater customer concentration, and deteriorating inventory liquidity. Evidence reported by Liu et al., (2025) further demonstrates that network characteristics can either amplify or mitigate the effects of political risk misalignment, confirming that corporate exposure depends substantially upon relational architecture rather than firm-specific preparedness alone. The literature consequently challenges the conventional treatment of geopolitical risk as an external strategic variable. Its consequences increasingly penetrate procurement, inventory, financing, logistics, production, and customer relationships. Corporate vulnerability becomes more complex because a political disturbance can activate several interconnected exposures simultaneously, requiring risk management to evaluate transmission pathways across the complete business network. The strategic importance of logistics adaptability is illustrated by Liu et al., (2025) in the context of innovation and global shipping operations. Geopolitical assessment is stronger when managers trace how political disruption moves through suppliers, financing, inventory, logistics, and customer relationships instead of treating each exposure as a separate entry.

2.3 Digital Dependence Escalating Cyber Risk Technology Vulnerability

Digitalisation has fundamentally altered the architecture of corporate exposure by making organisational performance increasingly dependent upon information systems, cloud services, connected infrastructure, external technology providers, and digitally enabled supply networks. Cyber risk therefore extends beyond the conventional protection of internal information technology assets. Latsiou and Lambrinoudakis (2026) show that contemporary cyber supply chain risk encompasses manufacturers, system integrators, ICT service providers, and digital service providers, creating vulnerabilities that organisations may struggle to observe because critical technologies are frequently sourced externally. Their review also demonstrates that IT outsourcing and accelerated digital adoption have increased concern regarding risks embedded within products and services over which purchasing organisations possess limited visibility. Seid et al., (2025) similarly examine ISO, NIST, and NIS2 approaches to cyber supply chain resilience and emphasise the growing importance of third-party risk management as cyber attacks increasingly threaten organisational integrity and data security. Cyber vulnerability is consequently becoming relational. Security weaknesses within suppliers, platforms, software components, or external service providers can create operational consequences for organisations whose own internal security arrangements remain comparatively strong. Digital risk assessment should identify which external platforms, providers, data flows, and system interfaces could interrupt critical operations, then evaluate how quickly those failures could spread. Risk ownership therefore needs to extend across functional boundaries so that early warning information can be translated into coordinated operational and strategic action.

Artificial intelligence introduces an additional layer of complexity because technology can simultaneously reduce and create business risk. Emerging research on supply chain cyber risk indicates that AI capabilities can support different stages of cyber risk management, creating opportunities to improve detection, analysis, and response. However, technological sophistication

does not automatically translate into lower organisational exposure. McLemore and Mihov (2026) examine AI investment and operational losses among large United States bank holding companies and report that greater AI investment can be associated with higher operational losses, particularly through external fraud, client related problems, and system failures, with stronger effects where risk management practices are weaker. Latsiou and Lambrinoudakis (2026) further demonstrate that digital supply chains expose firms to risks originating from technologies and providers beyond their direct control. These findings reveal a significant paradox within the next generation of business risk. Technology strengthens predictive capability, automation, visibility, and responsiveness while simultaneously creating dependencies that can enlarge the organisational attack surface and introduce new failure pathways. Digital transformation should therefore be evaluated not merely according to productivity gains but according to the additional technological concentration, third-party exposure, system interdependence, and operational vulnerability it creates. Cyber governance becomes effective when technology, procurement, operations, compliance, and executive management share responsibility for translating warning signals into coordinated action. Such coordination can reveal hidden downstream effects early enough for management to contain a supplier or system weakness before it becomes a wider corporate disruption.

2.4 Climate Exposure Transforming Environmental Risk Corporate Vulnerability

Climate related uncertainty has evolved from a predominantly environmental concern into a multidimensional source of corporate vulnerability with implications for financial markets, operational continuity, strategic investment, governance, and supply networks. Naseer et al., (2025) demonstrate through international evidence that corporate climate risk exposure increases market volatility, while stronger corporate governance and greater research and development intensity can moderate these effects. Qiu et al., (2025) similarly find that corporate climate risk exposure reduces stock liquidity and that transition risk produces a particularly pronounced negative effect, with subsequent implications for firm performance. Climate risk therefore reaches considerably further than direct physical damage from extreme weather. Regulatory transition, technological substitution, investor expectations, energy restructuring, and changing environmental policies can influence financing conditions and strategic competitiveness even where physical assets remain unaffected. Hou et al., (2025) conceptualise this challenge through corporate strategic responses to climate risk exposure, distinguishing between defensive reactions and more active forms of strategic integration. The emerging literature consequently positions climate exposure as a strategic business risk whose consequences depend upon both the external intensity of environmental change and the internal capacity of organisations to incorporate that change into corporate decision making. Related evidence from Hosseini Shekarabi et al., (2025) shows how intermodal transport strategy exposes firms to both network innovation and cross-border coordination challenges. Climate analysis should therefore connect physical hazards and transition pressures with financing, asset utilisation, supplier continuity, insurance, and strategic investment consequences.

The network dimension of climate exposure further demonstrates why environmental risk should not be assessed independently from other sources of business vulnerability. Research on global energy companies finds that green energy supply chain vulnerability amplifies corporate climate risk exposure and identifies governance quality as an important mechanism for mitigating these effects. Qiu et al., (2025) provide another governance perspective by demonstrating that interactions between investors and firms concerning environmental concerns can reduce corporate climate risk

exposure, indicating that external stakeholder scrutiny can influence organisational responses. Naseer et al., (2025) similarly establish that corporate governance moderates the relationship between climate risk and market volatility, strengthening the argument that vulnerability is shaped by governance capability as well as environmental conditions. Evidence across 2,146 nonfinancial firms in 34 countries further shows that climate change risk is positively associated with corporate risk taking, while board gender diversity and ESG performance moderate this relationship. Climate risk therefore interacts with governance, investment, liquidity, supply networks, and corporate behaviour. Environmental exposure becomes particularly dangerous where these interactions are overlooked, because organisations may manage sustainability indicators successfully while remaining financially or operationally vulnerable to the wider transmission effects of climate change. The managerial challenge is not simply to predict the next event, but to understand which organisational structures can amplify its consequences and which capabilities can contain them.

2.5 Interconnected Risk Elevating Strategic Organisational Resilience Imperatives

Resilience has emerged as a central response to next generation business risk because complete prediction becomes increasingly unrealistic as the number and interdependence of threats expand. Contemporary research distinguishes resilience from conventional risk prevention by emphasising the organisational capacity to absorb disruption, maintain critical functions, recover performance, and adapt structures after significant change. Hosseini Shekarabi et al., (2025) identify three major research clusters involving optimisation for resilience, technology adoption, and strategies addressing disruption and risk management, demonstrating the multidisciplinary character of contemporary resilience research. Paul and Saha (2025) likewise emphasise flexible strategies and performance indicators as important components of supply chain resilience, reinforcing the importance of organisational flexibility under conditions of disruption. Monazzam and Crawford (2024) extend this reasoning beyond supply chains by demonstrating how enterprise risk management practices can develop and sustain resources and capabilities required for organisational resilience during strategic transformation. These studies collectively suggest that effective risk management cannot depend entirely upon identifying every possible threat before it occurs. Firms require capabilities that remain useful even where the precise source, timing, or combination of disruption is uncertain. Consequently, resilience depends on combining analytical intelligence with governance arrangements that preserve accountability, flexibility, and timely intervention when conditions change. Embedding resilience indicators in ordinary planning helps organisations detect declining substitution capacity, tightening liquidity, supplier fragility, or digital dependence before these weaknesses combine during disruption.

A deeper distinction is emerging between restoring previous performance and transforming organisational structures in response to fundamentally altered risk conditions. Abudu et al., (2025), covering 52 empirical studies, 236 independent samples, and 22,955 observations, differentiate adaptive resilience, which emphasises rapid recovery, from transformative resilience, which involves longer term structural adaptation. Dahmen (2023) similarly argues that resilience has become an essential property of enterprise risk management in environments characterised by novel and severe crisis events. Chang et al., (2025) provide empirical support for the continuing importance of resilience by demonstrating that geopolitical risk weakens global supply chain resilience through mechanisms including trade credit and inventory costs. Chang et al., (2025) demonstrate that geopolitical exposure can weaken resilience, while Liu et al., (2025) additionally show that network

configuration can alter the resilience consequences of political risk perception. Taken together, the literature indicates that corporate vulnerability cannot be managed effectively through larger inventories of individual risks alone. The strategic requirement is an integrated capability to detect interconnected exposures, absorb shocks, coordinate responses, preserve critical operations, and transform organisational structures where returning to previous conditions would merely reproduce the vulnerabilities that created the disruption. Digital risk is further illustrated by Seid et al., (2025), who identify system maintenance and security as material concerns in smart warehouse technology integration.

3. SYSTEMIC VULNERABILITIES RESHAPING EMERGING BUSINESS RISK LANDSCAPES

The contemporary risk environment is challenging the assumption that corporate threats can be separated into stable categories and managed independently through specialised functions. Increasing connectivity across financial markets, digital infrastructure, supply networks, geopolitical systems, environmental conditions, and regulatory environments means that disruption originating in one domain can rapidly penetrate several others. Abdelhedi and Ben Hamida (2026) demonstrate persistent relationships among geopolitical risk, supply chain pressure, and large firm volatility, illustrating how external instability can migrate into corporate financial exposure. Malik and Terzidis (2026) similarly show that resilience and strategic adaptation have become increasingly important as global businesses confront geopolitical uncertainty and turbulent operating conditions. Monazzam and Crawford (2024) further establish that enterprise risk management contributes to organisational resilience when risk governance, awareness, culture, and strategic transformation are integrated rather than managed as disconnected activities.

3.1 Geopolitical Risk Escalating Enterprise Wide Business Vulnerability

Political instability can no longer be treated as a distant external variable monitored primarily by multinational strategy teams. Trade disputes, sanctions, diplomatic tensions, military conflict, protectionism, and changing international alliances can rapidly influence procurement, supplier availability, transportation, financing, investment, inventory, and market access. Abdelhedi and Ben Hamida (2026) demonstrate that geopolitical risk and supply chain pressure are dynamically connected with the volatility of major firms in the United States, China, and Japan, providing evidence that political uncertainty can migrate directly into corporate financial exposure. Wang and Wang (2025) similarly find that geopolitical risk exacerbates corporate maturity mismatch by increasing long-term investment and short term borrowing while simultaneously increasing information asymmetry and default risk. The significance of these findings lies in the multidimensional character of the resulting vulnerability. An international conflict may initially appear to represent political risk, yet its consequences can become liquidity risk, supplier risk, market risk, financing risk, or operational risk within a short period. Businesses that continue assigning geopolitical exposure exclusively to strategic planning functions may therefore underestimate the speed and breadth through which political disturbances can alter their internal risk profile. No single geopolitical safeguard is sufficient when exposure is distributed across suppliers, transport routes, financing arrangements, customers, and regulatory jurisdictions. Managers should therefore map the business pathways through which a political shock can alter procurement, liquidity, inventory availability, logistics continuity, and market access.

Corporate exposure becomes even more difficult to manage where international operations depend on extensive supplier networks that cross politically sensitive jurisdictions. Yu et al., (2025), examining United States multinational subsidiaries operating in China, demonstrate that resilience under geopolitical tension develops through different trajectories involving resistance, adaptation, and organisational learning. Firms capable of deeper adaptation can move beyond recovery towards stronger post-disruption positions, whereas defensive responses may merely restore previous conditions. Liu et al., (2025) further show that rising political disagreement and country specific geopolitical risk influence the foreign supplier choices of United States firms, confirming that geopolitical conditions increasingly affect sourcing architecture. Internationally scaling businesses may be especially vulnerable because they frequently possess fewer resources and less resilience than established multinational enterprises while remaining highly exposed to techno nationalism, trade protectionism, and geopolitical tension. These findings indicate that geopolitical risk is becoming structurally embedded within global business networks. The critical issue is consequently not whether firms can predict the next political crisis, but whether their supply, financial, operational, and market configurations are sufficiently adaptable to absorb geopolitical shocks without creating disproportionate corporate instability. Geopolitical analysis should concentrate on how disruption propagates through network structure, especially where several apparently independent suppliers share the same jurisdiction, infrastructure, or upstream source. Assessment should test whether alternative suppliers, routes, financing options, inventory buffers, and customer channels can absorb a political shock before instability becomes enterprise-wide.

3.2 Artificial Intelligence Accelerating Risks Exceeding Existing Control Capacity

Technological innovation presents an unusual risk paradox because the same capabilities that improve prediction, automation, and decision efficiency can create new forms of operational exposure. Artificial intelligence increasingly supports fraud detection, customer interaction, financial analysis, resource allocation, cybersecurity, and strategic decision making, yet its integration can also create model failure, data dependency, external provider concentration, inaccurate outputs, system instability, and governance uncertainty. McLemore and Mihov (2026), using supervisory data from large United States bank holding companies, find that greater AI investment is associated with higher operational losses per dollar of assets, particularly through external fraud, client related problems, and system failures. The risk enhancing relationship is stronger among institutions with weaker risk management practices. Szadeczky and Bederna (2025) similarly demonstrate that AI applications operate across highly varied risk profiles and therefore require differentiated approaches to risk assessment, regulation, and governance rather than universal controls. These findings challenge the assumption that technological sophistication automatically improves corporate control. AI can strengthen an organisation's capacity to manage uncertainty while simultaneously creating vulnerabilities that conventional operational risk frameworks were not originally designed to identify, measure, or contain. At the firm level, Yusof (2025a) shows that technology adoption can influence growth, innovation, and digital sustainability, reinforcing the need to govern technological dependence carefully. AI governance should identify model, data, provider, infrastructure, and specialist-skill dependencies because failures in these areas can move rapidly from technical malfunction into operational and financial loss.

An additional complication arises from the regulatory, ethical, and decision risks generated by increasingly autonomous systems. Orwat et al., (2024) demonstrate that risk-based AI regulation

requires organisations and regulators to make difficult normative judgements concerning fairness, privacy, acceptable risk, standardisation, and competing societal values. Rajendra and Thuraisingam (2026) similarly identify explainability and meaningful human intervention as central concerns where AI supported decisions affect rights and opportunities, particularly because opaque models can complicate accountability and legal scrutiny. Taeihagh (2025) argues that generative AI introduces governance challenges involving data, intellectual property, control, technical capability, and rapidly evolving regulation, requiring more adaptive approaches to technological governance. Ulnicane (2025) further demonstrates that generative AI governance is shaped by multiple centres of authority and competing interests rather than by technical risk considerations alone. Earlier analysis by Veale and Zuiderveen Borgesius (2021) also shows that risk-based AI regulation can generate important enforcement and implementation challenges. The emerging business problem is therefore multidimensional: AI risk simultaneously concerns technology, operations, regulation, accountability, reputation, and organisational judgement. AI warning signals require defined escalation routes linking technical teams, risk managers, legal specialists, business owners, and senior decision makers so that accountability remains clear when automated systems fail. Early visibility of indirect effects enables management to intervene before localised disruption spreads into wider enterprise vulnerability. Treating AI risk as an enterprise governance problem clarifies how model behaviour, regulatory exposure, customer harm, reputation, and operational continuity can become connected consequences of the same technological decision.

3.3 Cyber Risk Expanding Entire Business Ecosystem Vulnerability

Cybersecurity exposure is becoming increasingly difficult to contain because digital interdependence extends far beyond an organisation's own information systems. Contemporary businesses depend on cloud infrastructure, outsourced software, digital platforms, payment providers, data processors, technology suppliers, and interconnected operational systems, meaning that a cyber weakness outside the organisation can interrupt services inside it. Latsiou and Lambrinoudakis (2026) demonstrate that cyber supply chain risk increasingly encompasses manufacturers, system integrators, information and communication technology providers, and digital service providers, making systematic identification and treatment of external vulnerabilities essential. Chung et al., (2025) similarly argue that rapidly changing operational environments are reducing the adequacy of traditional risk management approaches and increasing the importance of data-driven operational risk management. The critical vulnerability lies in visibility. Organisations can enforce strong cybersecurity controls over their own infrastructure while remaining exposed through suppliers whose practices, vulnerabilities, updates, or subcontractors are poorly understood. Digital dependence consequently converts cybersecurity from an internal technology risk into a network risk capable of transmitting operational disruption, financial losses, customer harm, regulatory consequences, and reputational damage across multiple organisations simultaneously. Mapping secondary effects helps organisations detect escalation pathways before isolated disruption becomes a broader corporate problem. The managerial priority is therefore to identify organisational structures that amplify disruption and capabilities capable of containing its consequences.

Third party concentration further magnifies this exposure because numerous organisations may depend on the same technology providers, software components, or cloud infrastructure. A disruption affecting one critical provider can therefore generate simultaneous consequences across customers, sectors, and markets. This creates risk characteristics closer to systemic vulnerability than

conventional isolated cyber incidents. Latsiou and Lambrinoudakis (2026) emphasise that organisations increasingly acquire technologies and digital services from external providers while lacking complete visibility into the security conditions embedded within these supply relationships. The wider AI governance literature reinforces this concern because advanced digital systems increasingly rely on interconnected datasets, computational infrastructure, third-party models, and software ecosystems. Orwat et al., (2024) demonstrate that emerging technology risks can be difficult to quantify because risk assessment itself involves choices concerning what harms should be measured and which levels of exposure should be considered acceptable. Szadeczky and Bederna (2025) similarly argue that risk management should reflect the characteristics of particular technological applications rather than rely on uniform assumptions. The central issue is that firms increasingly control only a portion of the digital ecosystem upon which their continuity depends, creating a growing gap between operational responsibility and technological control. The accountability dimension is consistent with Gleißner and Berger (2024), who position embedded risk governance as a foundation of stronger organisational decision making. For cyber risk, strategic awareness improves when technical indicators are interpreted alongside service continuity, supplier dependence, regulatory exposure, customer trust, and potential financial loss.

3.4 Climate Risk Converging Financial Operational Strategic Exposure

Environmental disruption is increasingly demonstrating that climate risk cannot be confined to sustainability reporting or environmental management functions. Physical events such as extreme weather, heat, flooding, drought, and resource scarcity can affect facilities, transportation, energy availability, workforce productivity, supplier continuity, and inventory flows, while transition risks arising from regulation, changing technologies, financing conditions, and customer expectations can reshape long-term competitiveness. Naseer et al., (2025), using 38,808 firm year observations across 54 countries, find that greater corporate climate risk exposure significantly increases market volatility. They further show that stronger corporate governance and greater research and development intensity can mitigate this relationship, while weaker institutional environments can amplify it. Wang et al., (2025) provide complementary evidence that geopolitical risk can increase firm level climate risk exposure through channels including cash flow volatility, financing constraints, and leverage, demonstrating that environmental vulnerability may itself be intensified by other forms of uncertainty. Climate exposure should therefore be understood as a transmission risk capable of moving simultaneously through physical assets, supply networks, financing arrangements, market expectations, and strategic investment decisions. Resilience therefore requires analytical intelligence supported by governance arrangements that maintain accountability, flexibility, and timely intervention under changing conditions. Routine planning that incorporates interconnected exposure can reveal weak signals before they combine into material operational and financial pressure.

The increasing interaction between climate risk and corporate responses creates another managerial difficulty because actions taken to reduce one form of exposure can influence others. Wang et al., (2025) show that AI adoption can enhance corporate ESG performance through financing constraint alleviation, improved external oversight, and stronger information disclosure, illustrating how technological capability can contribute to sustainability management. Wang et al., (2025) similarly find that artificial intelligence can strengthen corporate climate risk information disclosure by reducing agency costs and financing constraints while improving predictive capability. Yet

technology itself creates energy, cyber, governance, and operational dependencies, meaning that digital solutions cannot be assumed to reduce overall risk automatically. Climate change risk has also been shown to influence corporate risk taking across an international sample of firms, while board characteristics and ESG performance moderate this relationship. The emerging issue is therefore not simply how organisations should manage climate risk, but how they can determine the net effect of responses that alter financial, technological, operational, and environmental exposures simultaneously. Corporate vulnerability increasingly depends on interactions among risk categories rather than on environmental conditions considered independently. Integrating these factors into regular planning allows organisations to detect early warning patterns before vulnerabilities become mutually reinforcing. No single safeguard should be treated as sufficient because its effectiveness is shaped by the broader system in which the control operates.

3.5 Isolated Risk Preparation Weakening Organisational Resilience Capacity

Risk management becomes strategically inadequate when organisations maintain sophisticated controls for individual threats but lack the capability to manage simultaneous or cascading disruption. A firm may possess strong cyber controls, diversified suppliers, insurance coverage, financial reserves, and climate policies while remaining vulnerable if those mechanisms are designed independently and cannot coordinate under pressure. Hosseini Shekarabi et al., (2025), reviewing 294 peer-reviewed studies, identify optimisation, technology adoption, disruption management, and resilience strategies as interconnected research clusters, indicating that modern resilience depends on combinations of managerial and technological capabilities. Monazzam and Crawford (2024) similarly demonstrate that enterprise risk management supports organisational resilience through risk governance, culture, awareness, strategic alignment, and capabilities that develop over time. Malik and Terzidis (2026) further show that strategic adaptation has become increasingly important for businesses operating under geopolitical turbulence, where static responses are unlikely to remain effective as environmental conditions evolve. The principal weakness of traditional preparedness is therefore fragmentation. Organisations can become highly capable at managing familiar risks independently while remaining poorly equipped for combinations of events that cross departmental, geographical, and technological boundaries. Transparency also matters because Gleißner and Berger (2024) associate stronger corporate transparency with organisational performance in listed companies. Systemic analysis reduces false confidence in isolated controls by recognising that protection depends on connected processes, partners, and infrastructure.

A further limitation emerges when resilience is interpreted narrowly as the ability to restore previous operations after disruption. Returning quickly to the pre-crisis state may be ineffective where that state contained the vulnerabilities responsible for the disruption. Yu et al., (2025) distinguish between stabilising and transformative resilience among multinational subsidiaries exposed to geopolitical tensions. Their findings indicate that deeper organisational learning and proactive adaptation can enable firms to emerge from disruption in a stronger configuration rather than merely recreating previous operating conditions. Malik and Terzidis (2026) similarly position resilience alongside strategic adaptation, emphasising the importance of organisational responses capable of evolving under continuing turbulence. Operational resilience research also stresses scenario planning, risk culture, information technology, tolerance setting, and maturity assessment as important components of preparing firms for significant disruptions. The next generation of business risk therefore exposes a critical resilience gap. Firms require more than inventories of risks and

recovery plans. They need the capability to recognise interdependencies, anticipate transmission pathways, coordinate responses across organisational boundaries, learn from disruption, and redesign structures before repeated shocks transform temporary exposure into persistent corporate vulnerability. Practical risk assessment must examine how exposures migrate across organisational systems instead of treating categories as self-contained. Risk analysis should consequently map critical dependencies, concentration points, response capacity, and propagation speed across the wider operating network.

4. INTERCONNECTED RISK PATHWAYS RESHAPING CORPORATE VULNERABILITY DYNAMICS

Corporate vulnerability increasingly reflects the interaction of multiple exposures rather than the isolated effect of a single threat. Geopolitical instability can alter sourcing decisions, increase inventory requirements, restrict financing, disrupt transportation, and weaken customer relationships, while technological dependence can strengthen operational efficiency yet simultaneously introduce cyber exposure, third-party concentration, and system failure risks. Chang et al., (2025) demonstrate that geopolitical risk weakens global supply chain resilience through reduced trade credit and increased inventory costs, providing clear evidence that political uncertainty can migrate into financial and operational systems. Xiong and Sun (2025) similarly show that geopolitical crises increase supply chain risk through resilience erosion, customer concentration, and deterioration in inventory liquidity. Digital transformation adds another layer of complexity because it can reduce certain vulnerabilities while creating new dependencies. Recent evidence shows that digital transformation can help firms withstand uncertainty-driven supply shocks, even though macroeconomic uncertainty continues to increase disruption risk and weaken investment and output growth. These relationships suggest that modern risk management should focus less on constructing longer inventories of separate risks and more on understanding how threats move across functions, networks, technologies, and markets. The next generation of corporate vulnerability is therefore defined by connectivity, transmission, and amplification.

4.1 Geopolitical Risk Transmitting Multidimensional Business Function Vulnerability

Political disturbances increasingly acquire economic significance through the pathways connecting international events with ordinary corporate activities. A conflict or diplomatic dispute may originate outside the organisation, but its consequences can penetrate procurement, logistics, working capital, pricing, customer demand, and investment decisions within a relatively short period. Chang et al., (2025) find that geopolitical risk significantly reduces global supply chain resilience and identify decreased trade credit and increased inventory costs as important mechanisms through which that effect occurs. Such evidence demonstrates that political uncertainty should not remain confined to strategic environmental scanning because its impact ultimately becomes operational and financial. Xiong and Sun (2025) reach a complementary conclusion, showing that geopolitical crises increase supply chain risk through reduced resilience, greater customer concentration, and weaker inventory liquidity. This transmission process is particularly important for internationally connected firms because conventional country risk assessments may capture the location of exposure without adequately explaining its corporate consequences. Managers consequently need to understand not only which markets or countries are politically unstable, but also which suppliers, customers, financing arrangements, inventories, and operational processes depend upon those environments. Political risk becomes strategically significant precisely because its effects rarely remain political

once they enter the organisation. Geopolitical transmission mapping should show which suppliers, corridors, working-capital arrangements, inventory policies, and customer markets would be affected first, together with the organisation's available alternatives.

Network structures further intensify this problem because contemporary firms depend on commercial relationships extending far beyond their direct visibility. Immediate suppliers may operate in politically stable locations while depending upon upstream materials, logistics corridors, technologies, or manufacturers exposed to geopolitical instability elsewhere. Chang et al., (2025) demonstrate that institutional conditions influence the severity of geopolitical effects on supply chain resilience, with weaker property rights protection amplifying vulnerability. Xiong and Sun (2025) similarly identify corporate characteristics that alter exposure, including political connections that can buffer the consequences of geopolitical crises. The broader implication is that geopolitical risk management should progress from geographical mapping towards dependency mapping. Organisations need visibility into the commercial pathways through which a political event can alter material availability, financing, supplier behaviour, customer concentration, and inventory requirements. Risk assessment should therefore incorporate indirect dependencies and secondary effects rather than concentrate exclusively on direct operations within high-risk jurisdictions. Such an approach would also strengthen scenario planning because management could evaluate how geopolitical shocks propagate through different organisational systems. The strategic challenge is not merely predicting where political instability will occur, which remains inherently difficult, but designing business structures capable of absorbing its consequences without allowing a localised geopolitical disturbance to evolve into a broader corporate crisis. This governance perspective is reinforced by Monazzam and Crawford (2024), who examine the performance relevance of corporate governance transparency.

4.2 Technology Delivering Protection While Creating Emerging Corporate Exposure

Digital transformation deserves a more balanced interpretation within risk management because technological sophistication does not automatically produce stronger organisational resilience. Advanced analytics, artificial intelligence, cloud platforms, automation, and interconnected information systems can improve forecasting, visibility, decision speed, and operational coordination, especially under uncertain conditions. Evidence from 2025 shows that digital transformation can mitigate the supply chain disruption risk generated by macroeconomic uncertainty, supporting the argument that digital capability can strengthen resilience. At the same time, dependence upon complex technologies introduces vulnerabilities that may not exist in less digitised operating models. Technology failures can interrupt production, compromise information, disrupt communications, affect customer service, and create dependencies upon providers whose internal controls remain outside the organisation's direct authority. Latsiou and Lambrinoudakis (2026) demonstrate that cyber supply chain risk increasingly arises from manufacturers, system integrators, ICT service providers, and digital service providers, particularly where organisations outsource technology and possess limited visibility into what they acquire. Consequently, digitalisation should not be assessed purely according to its contribution to productivity or resilience. Management should simultaneously evaluate what new failure points, dependencies, concentrations, and third-party exposures are created whenever technological capability becomes embedded within critical business processes. A technology investment should therefore be assessed for residual vulnerability, including provider concentration, recovery difficulty, data dependence, cybersecurity

exposure, and the consequences of prolonged service failure. This broader perspective improves strategic awareness by linking risk signals.

The relationship becomes even more complex because technology introduced to mitigate existing risk can generate secondary risk elsewhere in the organisation. Artificial intelligence may enhance threat detection, forecasting, or decision quality, while cloud platforms may strengthen scalability and disaster recovery, yet both can increase reliance on external infrastructure, data availability, software integrity, and specialist expertise. Contemporary cyber supply chain research shows that traditional supplier questionnaires and ratings are increasingly insufficient for identifying vulnerabilities in deeply interconnected digital ecosystems. The systematic review of cyber supply chain risk management published in 2026 similarly describes C SCRM as an increasingly important managerial imperative because interconnected supply chains are exposed to escalating cyber threats. These developments suggest that technological investment decisions should incorporate a broader concept of residual vulnerability. Managers need to assess whether the resilience benefits created by a new technology exceed the additional exposures created through system concentration, provider dependence, cybersecurity requirements, data governance, and operational complexity. This does not imply restricting innovation. Instead, technological resilience should be designed alongside technological adoption. Organisations that build redundancy, alternative service arrangements, stronger vendor governance, recovery mechanisms, and continuous monitoring into digital transformation are more likely to capture technological value without allowing efficiency improvements to conceal an expanding infrastructure of corporate vulnerability. Management needs less emphasis on precise event prediction and greater understanding of structures that magnify disruption or constrain its spread.

4.3 Cyber Risk Creating Enterprise Supply Network Dependency

Cyber exposure has expanded beyond the boundaries of internal information security because organisational continuity increasingly depends upon interconnected digital relationships. Firms rely on external software, cloud infrastructure, payment platforms, data processors, technology vendors, and digitally enabled suppliers, meaning that cyber incidents can originate in organisations with which the affected firm has little operational control. Latsiou and Lambrinoudakis (2026) show that cyber supply chain risk management must consider diverse supplier categories, including manufacturers, system integrators, ICT service providers, and digital service providers, because vulnerabilities can be embedded throughout the technology supply chain. The importance of this issue is reinforced by empirical evidence from Danish manufacturing SMEs. Research published in *Supply Chain Management: An International Journal* finds a positive indirect relationship between cybersecurity awareness and financial performance through cybersecurity supply chain risk management, suggesting that investment in C SCRM can produce business value rather than functioning solely as a technical security cost. These findings encourage a broader interpretation of cyber resilience. Protecting internal networks remains essential, but organisations must also understand how external technology dependencies influence critical operations. Cybersecurity therefore belongs within enterprise risk management because a serious cyber incident can create operational interruption, revenue loss, compliance exposure, supply failure, reputational damage, and strategic disruption simultaneously. The value of adaptive logistics strategy under disruption is also supported by Hosseini Shekarabi et al., (2025).

Greater interdependence also creates concentration risk because numerous organisations may depend upon the same technology provider or software component. A single failure can therefore produce cascading disruption across multiple firms and industries, transforming what appears to be a technology incident into a wider operational event. Latsiou and Lambrinoudakis (2026) note that recent supply chain attacks and operational failures have affected thousands of organisations and conclude that traditional supply chain risk methods are no longer sufficient on their own. This observation has important managerial consequences. Vendor due diligence cannot remain an occasional procurement exercise based predominantly on questionnaires, certifications, or contractual assurances. Critical digital suppliers should be subjected to continuous risk evaluation, dependency mapping, recovery testing, and contingency planning. Organisations also need to distinguish between replaceable digital services and dependencies whose failure would immediately interrupt core activities. The latter require stronger governance, alternative arrangements, and executive oversight. Cyber resilience thus depends as much on organisational architecture as on technical protection. Firms that understand which digital relationships are indispensable, how quickly they can substitute providers, where critical data reside, and how operations can continue during technology failure will be better positioned to manage the systemic character of modern cyber risk. Continuous incorporation of these factors strengthens early detection before separate pressures converge into significant corporate exposure.

4.4 Climate Exposure Multiplying Corporate Risk Vulnerability Dynamics

Climate related disruption demonstrates why conventional boundaries between environmental, financial, operational, and strategic risk are becoming increasingly difficult to preserve. Extreme weather can damage physical facilities, interrupt transportation, reduce workforce productivity, destabilise energy supply, and constrain material availability, while transition pressures can alter regulation, technology investment, consumer expectations, and financing conditions. The significance of climate risk therefore lies not simply in environmental harm but in the diversity of corporate consequences it can produce. Businesses that continue treating climate exposure primarily as a sustainability reporting matter risk overlooking its potential to disrupt ordinary commercial activity. This becomes particularly important for organisations operating complex supply networks because environmental events affecting distant suppliers or infrastructure can produce indirect operational consequences even when the firm's own facilities remain unaffected. The emerging business risk landscape therefore requires climate considerations to be embedded within investment appraisal, supplier evaluation, continuity planning, insurance, financing strategy, and capacity decisions rather than managed separately from mainstream corporate risk. Such integration would also allow organisations to evaluate how climate adaptation decisions interact with other vulnerabilities, including technology dependence, supplier concentration, energy cost, and regulatory exposure. Control effectiveness must be judged within the wider dependency network rather than assessed as an isolated protective mechanism. Climate risk assessment should trace how a physical or transition event can move through production, transport, energy, insurance, financing, supplier performance, and market demand.

Environmental risk also illustrates the importance of distinguishing direct exposure from systemic vulnerability. A company may not possess assets in locations experiencing severe physical climate events but may still depend on suppliers, transport routes, commodities, utilities, or customers affected by those conditions. This indirect exposure resembles the network transmission observed in

geopolitical and cyber risk, reinforcing the need for risk management to focus on dependency structures. Corporate responses should therefore extend beyond individual site protection towards broader assessments of supply continuity, material substitution, energy resilience, insurance availability, and financial flexibility. This interpretation also strengthens the case for integrated scenario analysis. Management should evaluate combinations of environmental and economic pressures, such as extreme weather occurring during periods of high borrowing costs, constrained inventories, or geopolitical disruption. Such combinations may create significantly greater vulnerability than any individual event considered independently. Climate risk consequently functions as a corporate risk multiplier because it can intensify operational weaknesses that already exist within the organisation. Firms with concentrated sourcing, low liquidity, fragile infrastructure, or limited alternative capacity are likely to experience greater consequences from similar environmental shocks. Climate resilience therefore depends on the quality of the broader corporate architecture through which environmental exposure is absorbed and managed. Technology-enabled resilience is further reflected in Hosseini Shekarabi et al., (2025), who link warehouse management systems with supply chain resilience and business competitiveness.

4.5 Transformative Resilience Replacing Recovery Centric Structural Responses

The growing interconnection among contemporary risks makes recovery alone an insufficient measure of organisational resilience. Traditional continuity planning frequently evaluates resilience according to how rapidly operations return to normal following disruption. This remains useful where shocks are temporary and underlying business conditions remain stable. However, restoring the previous operating model can reproduce the same vulnerabilities if the external environment has changed permanently. Research on geopolitical risk illustrates this problem clearly. Chang et al., (2025) show that political uncertainty can weaken supply chain resilience through higher inventory costs and tighter trade credit, while Xiong and Sun (2025) identify resilience erosion, customer concentration, and inventory liquidity as important transmission channels. These mechanisms may require structural changes rather than temporary recovery actions. Supplier diversification, revised inventory policies, alternative financing arrangements, regionalised production, or redesigned customer portfolios may become necessary if geopolitical instability persists. Likewise, cyber vulnerabilities may require changes to technology architecture rather than simply restoring systems after an incident. Resilience should therefore be assessed according to whether the organisation can adapt its configuration in response to changing risk conditions, not merely whether it can resume previous activities after interruption. Resilience assessment should identify which dependencies would force structural change after disruption and which resources can be substituted quickly enough to preserve critical operations. Organisations should distribute risk accountability across relevant functions, allowing emerging signals to be converted rapidly into coordinated operational and strategic decisions.

Structural adaptation inevitably requires firms to reconsider the longstanding emphasis on maximum efficiency. Lean inventories, concentrated suppliers, extensive outsourcing, centralised technology platforms, and tightly integrated networks can generate substantial economic benefits during stable periods, yet they may also reduce strategic flexibility when disruption becomes persistent. Evidence from geopolitical supply chain research illustrates these tradeoffs because heightened uncertainty can increase precautionary inventory costs while simultaneously constraining trade credit. Economic

uncertainty research similarly shows that supply disruptions can weaken investment and output growth, although digital transformation can strengthen firms' capacity to absorb such shocks. Resilience therefore requires selective redundancy rather than indiscriminate duplication. Organisations need to determine which resources, suppliers, technologies, financial buffers, and capabilities justify additional capacity because their failure would create disproportionate strategic consequences. Such decisions should be informed by criticality and interconnectedness rather than cost alone. A resilient organisation is not necessarily one that maintains the largest buffers, but one that knows where flexibility matters most. The strategic objective is to develop sufficient adaptive capacity to redesign vulnerable arrangements before repeated disruption converts temporary operational problems into persistent corporate weakness. Functional boundaries should not obstruct risk escalation; emerging signals must reach decision makers capable of coordinating operational and strategic responses. This approach distinguishes temporary interruption from structural weakness and gives management a clearer basis for deciding when recovery is insufficient and redesign is necessary.

5. STRATEGIC ARCHITECTURE STRENGTHENING NEXT GENERATION RISK RESILIENCE

The increasing interconnectedness of corporate exposure requires organisations to redesign risk management around vulnerability, adaptability, and strategic resilience rather than relying predominantly on separate controls for individual threats. Traditional risk registers remain useful, but they are insufficient where geopolitical instability can trigger financing difficulties, supply interruption, inventory pressure, and market volatility simultaneously, or where digital solutions introduced to reduce operational risk generate additional cyber and technology dependencies. Monazzam and Crawford (2024) demonstrate that enterprise risk management can strengthen organisational resilience through risk governance, culture, awareness, and strategic alignment. Recent evidence further indicates that geopolitical risk can undermine supply chain resilience through trade credit and inventory cost channels, while macroeconomic uncertainty can increase disruption risk and weaken investment and output growth (Chang et al., 2025). Organisations should consequently progress towards an integrated architecture in which risk connectivity, critical dependencies, adaptive capacity, and potential cascading effects become central to managerial decision making. Five strategic priorities are particularly important: developing interconnected enterprise risk intelligence, redesigning networks against geopolitical concentration, governing digital and cyber dependencies, embedding climate exposure within corporate decisions, and institutionalising transformative resilience. Collectively, these priorities can shift risk management from defensive control towards an organisational capability capable of protecting continuity and strategic value under increasingly complex conditions.

5.1 Integrated Enterprise Risk Intelligence Architecture Capability Development

Organisations should replace fragmented risk visibility with an integrated intelligence architecture capable of identifying relationships among strategic, operational, financial, technological, geopolitical, cyber, and environmental exposures. Risk registers organised exclusively by departmental ownership can obscure transmission pathways because a threat classified within one function may create consequences across several others. Monazzam and Crawford (2024) demonstrate that enterprise risk management contributes to organisational resilience through the interaction of risk governance, awareness, culture, and strategic transformation, supporting a more

integrated approach to organisational preparedness. Liu et al., (2025) provide further evidence that risk awareness must extend beyond the focal organisation because misalignment in political risk perceptions between supply chain partners reduces operational resilience. Firms should therefore develop enterprise risk maps connecting critical assets, suppliers, customers, technologies, financing arrangements, infrastructure, geographical locations, and regulatory dependencies. Each major exposure should be evaluated according to direct impact, secondary consequences, propagation speed, dependency concentration, and recovery difficulty. Risk committees could supplement conventional probability and impact matrices with interconnected scenario analysis that examines combinations of threats rather than individual events. Such architecture would enable management to recognise that corporate vulnerability frequently develops through relationships among risks and could reveal concentrations that remain invisible within traditional functional reporting structures. The resilience implications of digital adoption are also visible in Yusof (2025b), particularly where smaller enterprises operate with constrained resources.

Risk intelligence should also become dynamic rather than being concentrated around annual risk assessments. Rapid changes in political conditions, cyber threats, technologies, climate exposure, and economic uncertainty can render static assessments obsolete long before formal review cycles are completed. Malik and Terzidis (2026) emphasise resilience and strategic adaptation as critical organisational responses to geopolitical turbulence, demonstrating the importance of continuous adjustment under unstable global conditions. Wang and Wang (2025) show that geopolitical risk can exacerbate corporate maturity mismatch by affecting investment and financing structures, illustrating how external uncertainty can penetrate decisions that might otherwise be considered purely financial. Xiong and Sun (2025) similarly identify resilience erosion, client concentration, and deteriorating inventory liquidity as pathways through which geopolitical crises increase supply chain risk. Management dashboards should consequently integrate leading indicators covering political exposure, supplier concentration, cyber incidents, liquidity conditions, climate vulnerability, critical technology dependencies, and operational disruption. Escalation thresholds should be established for situations in which changes across several indicators suggest accumulating systemic vulnerability. This approach would transform risk management from retrospective reporting into an anticipatory decision capability, enabling organisations to recognise emerging patterns before individual exposures converge into a major corporate disruption. Strategic preparedness depends on recognising which organisational arrangements intensify disruption and which capabilities can absorb or contain its effects. Strong resilience combines risk intelligence with governance mechanisms that preserve decision accountability, adaptive flexibility, and timely managerial intervention.

5.2 Supply Network Redesign Reducing Geopolitical Concentration Risk

Global sourcing strategies should be recalibrated to reduce excessive dependence on countries, suppliers, customers, transport corridors, and critical components whose disruption could destabilise entire operating systems. Cost efficiency should remain important, but sourcing decisions require explicit consideration of geopolitical concentration and network vulnerability. Chang et al., (2025) find that geopolitical risk significantly weakens global supply chain resilience, with reduced trade credit and increased inventory costs functioning as important transmission mechanisms. Cui et al., (2025) further demonstrate that sourcing decisions for critical components under supply risk are influenced by diversification and competition effects, reinforcing the strategic importance of

alternative supply configurations. Firms should therefore classify suppliers according to criticality, substitutability, geographical exposure, financial condition, technological dependence, and upstream concentration. Critical inputs should receive stronger resilience treatment through dual sourcing, regional alternatives, qualified backup suppliers, strategic inventory, flexible contracts, or reserved capacity where economically justified. Such measures should not be applied uniformly because indiscriminate redundancy can impose unnecessary costs. Instead, resilience investments should be concentrated on dependencies whose failure would generate disproportionate operational or financial consequences. This risk adjusted sourcing philosophy would preserve efficiency while preventing excessive concentration from becoming an invisible source of strategic fragility. Analytical capability creates greater resilience when governance also supports accountability, flexibility, and rapid intervention as conditions evolve. Routine supplier planning should therefore monitor common upstream dependencies, political exposure, substitution difficulty, transport alternatives, and financial fragility rather than relying only on first-tier supplier status.

Network redesign should extend beyond first tier suppliers because geopolitical vulnerability can remain hidden several layers upstream. A seemingly diversified procurement portfolio may still depend on common manufacturers, raw materials, technology providers, or logistics routes. Research on global supplier diversification demonstrates that improved information access can facilitate supplier search and broader diversification, thereby strengthening economic resilience. Liu et al., (2025) additionally show that network characteristics affect the resilience consequences of political risk perception, confirming that organisational exposure depends partly on the architecture connecting firms. Firms should consequently develop deeper supplier mapping for strategically important products and identify common dependencies across supposedly independent sourcing channels. Scenario analysis should test the consequences of simultaneous supplier failure, border restrictions, sanctions, transport disruption, commodity shortages, or sudden regulatory changes. Hybrid mitigation strategies are particularly valuable because resilience may require combinations of multisourcing, backup suppliers, regional sourcing, reserved inventory, excess capacity, and alternative transportation arrangements rather than reliance on one intervention. Research published in 2025 demonstrates that such combinations can be calibrated according to disruption probabilities and managerial risk tolerance. The strategic objective should not be complete insulation from geopolitical uncertainty, which is unrealistic, but a supply architecture capable of maintaining critical flows when established international relationships become temporarily or permanently unreliable. Leadership capability remains equally important, as Malik and Terzidis (2026) links digital and entrepreneurial leadership with organisational performance in emerging economies.

5.3 Digital Transformation Governance Managing Cyber Technology Dependence

Technology governance should evaluate digital capability and technological vulnerability as two dimensions of the same strategic decision. Organisations frequently assess digital investment according to efficiency, productivity, innovation, and customer value while cybersecurity and operational dependence are considered separately after implementation. This sequencing can allow new vulnerabilities to become embedded before risk controls are designed. Evidence indicates that digital transformation can reduce uncertainty-driven supply chain disruption by strengthening resilience, demonstrating its substantial protective value. Dong et al., (2025) similarly find that artificial intelligence is positively associated with supply chain resilience and can alleviate some adverse effects of geopolitical risk in high technology and highly competitive industries. Dong et

al., (2025) report that AI adoption can reduce supply chain risk through improved efficiency and resilience. These benefits should nevertheless be evaluated alongside the additional dependencies created by cloud platforms, algorithms, data infrastructure, software vendors, and external technology services. Every major digital investment should therefore undergo a technology resilience assessment covering criticality, data dependency, cyber exposure, provider concentration, recovery capability, interoperability, human override, and alternative operating arrangements before becoming deeply embedded within core business processes. Digital investment decisions should be judged across the complete technology ecosystem because strong internal controls cannot compensate for a critical external provider that lacks resilience. Before implementation, management should document how a platform, algorithm, cloud service, or data dependency could affect production, customers, compliance, and continuity if it becomes unavailable or compromised.

Cyber risk management should similarly expand from internal information security towards continuous governance of the entire digital supply ecosystem. Latsiou and Lambrinoudakis (2026) emphasise that outsourced technologies and services can expose organisations to vulnerabilities over which they possess limited visibility, requiring systematic cyber supply chain risk management. Seid et al., (2025) demonstrate the importance of ISO, NIST, and NIS2 frameworks for mitigating third-party cyber risks and strengthening supply chain resilience. Empirical evidence from Danish manufacturing SMEs further indicates that cybersecurity awareness can contribute indirectly to financial performance through stronger cybersecurity supply chain risk management practices. Firms should consequently classify digital vendors according to operational criticality and impose proportionate requirements involving security assessment, incident notification, recovery capability, subcontractor visibility, data portability, and continuity arrangements. Critical platforms should be tested through simulations involving provider outages, ransomware, corrupted data, connectivity failure, and compromised third parties. Particular caution is necessary with artificial intelligence because technological investment does not invariably reduce risk. McLemore and Mihov (2026) find that greater AI investment among large bank holding companies is associated with higher operational losses, especially where risk management practices are weaker. Digital resilience therefore requires governance that advances at the same speed as technological adoption. Cyber governance should therefore follow attack and failure pathways across vendors, subcontractors, shared infrastructure, data exchanges, and critical business services rather than assessing each digital asset in isolation.

5.4 Climate Exposure Integration Strengthening Financial Operational Strategic Decisions

Climate risk should be incorporated directly into enterprise risk management, capital allocation, supply chain design, financing decisions, and strategic planning rather than remaining predominantly within sustainability reporting. Physical and transition exposures can influence corporate performance through different channels, requiring firms to understand both immediate operational disruption and longer term economic consequences. Naseer et al., (2025), using evidence from 54 countries, find that greater corporate climate risk exposure increases market volatility, while stronger governance and research and development intensity can mitigate these effects. Qiu et al., (2025) similarly demonstrate that corporate climate risk exposure reduces stock liquidity and that transition risk produces a particularly pronounced negative effect. Climate exposure can therefore influence the organisation even without direct physical damage to its assets. Firms should establish climate risk assessments connecting facilities, suppliers, transport routes, commodities, energy requirements, insurance, financing, customers, and regulatory environments. Investment proposals

involving long lived assets should incorporate climate scenarios and transition assumptions rather than relying exclusively on historical conditions. Supplier assessments should also include physical exposure and adaptation capability because environmental disruption within upstream networks can create operational consequences for firms located far from the original climate event. Climate governance should identify where facilities, suppliers, transport routes, energy sources, commodities, insurance, and financing are concentrated, then test the organisation's capacity to respond under severe scenarios. Responsibility for climate exposure should link sustainability, finance, operations, procurement, risk, and strategy so that emerging physical or transition pressures influence decisions before losses become material.

Financial resilience should form a central component of climate adaptation because environmental exposure can constrain profitability, liquidity, and access to capital. Recent evidence indicates that firm level climate risk can weaken corporate resilience through reduced profitability and increased financing constraints, while financial flexibility can buffer negative climate shocks. Climate risk has also been shown to increase debt financing costs through market volatility, encouraging firms to accumulate cash reserves. Organisations should consequently align climate scenarios with liquidity planning, insurance strategy, capital expenditure, debt structure, and contingency reserves. Transparency should support this process rather than function solely as an external reporting requirement. Lei et al., (2025) find that climate risk disclosure can enhance stock liquidity, particularly where firms demonstrate stronger transparency and climate commitments. Wang et al., (2025) further show that artificial intelligence can improve corporate climate risk information disclosure by reducing agency costs and financing constraints while strengthening predictive capability. Climate governance should therefore combine disclosure with decision action. Organisations need mechanisms that convert environmental information into sourcing adjustments, asset protection, financing choices, technology investment, operational redesign, and strategic adaptation before climate exposure becomes financially material. Digital capability can also strengthen climate-related information disclosure and predictive assessment, as demonstrated by Wang et al., (2025). Financial climate indicators should therefore feed directly into capital allocation, liquidity planning, insurance decisions, supplier strategy, and asset protection rather than remain confined to disclosure processes.

5.5 Transformative Resilience Institutionalisation Strengthening Organisation Wide Adaptability

Organisations should redefine resilience as the capacity to adapt and transform vulnerable structures rather than merely restore operations after disruption. Conventional business continuity remains necessary, but returning quickly to a previous operating state may recreate the same weaknesses that made the organisation vulnerable initially. Malik and Terzidis (2026) position resilience alongside strategic adaptation in global business under geopolitical uncertainty, highlighting the importance of organisational responses that evolve with changing external conditions. Monazzam and Crawford (2024) similarly demonstrate that enterprise risk management can contribute to organisational resilience through governance, culture, strategic integration, and capability development. Chang et al., (2025) further demonstrate that geopolitical risk can significantly weaken global supply chain resilience through reduced trade credit and increased inventory costs, reinforcing the importance of strengthening adaptive organisational capabilities under persistent external uncertainty. Firms should therefore distinguish between recovery capability and transformative capability. Recovery

capability concerns restoring critical operations, while transformative capability involves redesigning suppliers, technologies, financing arrangements, processes, governance, or business models after evidence reveals structural weakness. Post disruption reviews should consequently examine more than response effectiveness. They should identify which organisational assumptions failed, which dependencies intensified losses, which controls proved inadequate, and which structural changes are required to prevent recurrence. Lessons should then be translated into investment priorities, operating policies, supplier strategies, technology architecture, and management accountability rather than remaining within incident reports.

Transformative resilience also requires a deliberate balance between efficiency and strategic flexibility. Excessive concentration, minimal inventory, single source procurement, extensive outsourcing, and dependence on common digital infrastructure may reduce costs during stable periods while increasing vulnerability under severe disruption. Supplier risk research published in 2026 emphasises that local supplier failures can propagate through networks and create system-wide consequences, reinforcing the importance of systematic supplier robustness assessment. Research on suppliers operating in politically unstable regions also demonstrates that governance mechanisms can function as dynamic adaptations balancing efficiency and adaptability, while trust does not necessarily strengthen resilience under every condition. Organisations should therefore identify critical activities where selective redundancy produces strategic value. Alternative suppliers, reserve capacity, financial buffers, backup technologies, decentralised decision authority, cross trained employees, and substitute logistics routes should be considered according to the consequences of failure rather than treated automatically as avoidable inefficiencies. Zhou and Zhao (2026) show that explainable machine learning can connect ESG performance, governance quality, financial flexibility, and supply chain structure with resilience prediction, supporting broader capability-based assessment. This approach would allow firms to invest selectively in flexibility where disruption could otherwise threaten continuity, profitability, or strategic survival. Rather than attempting perfect prediction, managers should identify amplification points and capabilities that limit the consequences of disruption. Resilience becomes more durable when risk intelligence is matched by governance capable of accountable, flexible, and timely action.

6. CONCLUSION

Corporate vulnerability is being redefined by a business environment in which disruption rarely remains confined to the domain in which it originates. Geopolitical instability can migrate into procurement, financing, inventory, logistics, and market exposure, while digital transformation can strengthen organisational capability and simultaneously create new technological dependencies, cyber vulnerabilities, and operational failure pathways. Climate disruption further intensifies this complexity by influencing physical assets, supply networks, financial conditions, investment priorities, and long-term competitiveness. The significance of these developments lies not simply in the emergence of additional risks, but in the increasing capacity of different threats to interact, transmit, and amplify their consequences across organisational boundaries. This interconnected character of contemporary exposure challenges conventional approaches that classify and manage risks as relatively independent categories. As established throughout this article, corporate vulnerability increasingly emerges from combinations of geopolitical, technological, cyber, environmental, operational, and financial pressures whose effects may develop simultaneously and reinforce one another. Risk management must consequently evolve from the control of identifiable

threats towards a more sophisticated understanding of the relationships, dependencies, and transmission mechanisms through which disruption can escalate into enterprise-wide instability.

A particularly important implication concerns the changing meaning of organisational resilience. Protection against future disruption cannot depend exclusively on forecasting individual threats or restoring operations to their previous condition after a crisis. The literature examined in this article positions resilience as a broader organisational capability involving the capacity to absorb shocks, preserve critical functions, coordinate responses, recover performance, and adapt organisational structures as risk conditions evolve. This distinction becomes critical because returning to an earlier operating configuration may simply recreate the vulnerabilities that allowed disruption to become severe in the first place. Organisations therefore require both adaptive and transformative capacity, supported by integrated risk intelligence, diversified supply arrangements, robust digital governance, climate responsive decision making, financial flexibility, and stronger visibility across critical dependencies. Such capabilities allow firms to move beyond reactive crisis management and confront uncertainty as a strategic condition that must be continuously interpreted and incorporated into corporate decisions. Resilience, from this perspective, is not merely the ability to survive disruption. It represents the organisational capacity to learn from exposure, redesign vulnerable structures, and preserve strategic viability as the nature of business risk continues to evolve.

The next generation of business risk ultimately demands a fundamental change in how organisations conceptualise vulnerability itself. A company may possess effective controls for individual risks and still remain highly exposed if management cannot recognise how suppliers, technologies, markets, financing structures, infrastructure, and external institutions connect those risks together. The article therefore advances an integrated and anticipatory perspective in which attention shifts from asking only what could go wrong towards understanding how disruption could travel through the organisation, what dependencies could magnify its consequences, and which capabilities would prevent localised failure from becoming systemic. This perspective is particularly important as organisations become more digitally connected, internationally interdependent, environmentally exposed, and reliant on networks extending beyond direct managerial control. Sustainable corporate resilience will consequently belong to organisations capable of combining foresight with adaptability, technological advancement with responsible governance, global connectivity with strategic diversification, and operational efficiency with sufficient flexibility to withstand profound uncertainty. The defining competitive advantage of the future may therefore rest not on eliminating risk, which remains impossible, but on constructing organisations sufficiently intelligent, resilient, and adaptable to prevent uncertainty from becoming vulnerability and vulnerability from becoming systemic failure.

DECLARATIONS

1. Acknowledgement

The authors gratefully acknowledge the academic support and resources provided by the Faculty of Business and Accountancy and the Institute of Graduate Studies, Universiti Poly-Tech Malaysia (UPTM). Appreciation is also extended to scholars whose published works provided important foundations for the conceptual examination of emerging business risks, corporate vulnerability, enterprise risk management, digital and cyber exposure, geopolitical uncertainty, climate risk, and organisational resilience.

2. Conflict of Interest

The authors declare that there are no financial, professional, or personal interests that could have influenced the preparation or publication of this article.

3. Author Contribution Statement

Nurul Najiha Abdulloh: Conceptualization, literature review, development of the conceptual arguments, manuscript preparation, and critical revision.

Shahri Abu Seman: Literature synthesis, conceptual development, scholarly interpretation, manuscript review, and refinement.

Zila Zainal Abidin: Conceptual development, critical evaluation, intellectual input, manuscript review, and refinement.

All authors reviewed and approved the final manuscript for publication.

4. Ethics Statement

This article is conceptual in nature and is based entirely on published scholarly literature. It does not involve human participants, surveys, interviews, experiments, or the collection of primary, confidential, or identifiable data. Therefore, institutional ethical approval and informed consent were not required. All scholarly sources were appropriately acknowledged and cited in accordance with established standards of academic integrity and responsible scholarly practice.

REFERENCES

- Abdelhedi, M., & Ben Hamida, L. (2026). Large firms' volatility, geopolitical risk, and supply chain pressure: A partial coherency and phase difference analysis. *Journal of Chinese Economic and Business Studies*, 24(2), 341–366. <https://doi.org/10.1080/14765284.2025.2601966>
- Abudu, R., Thompson, E. A., Dzawu, F. S., & Roa-Henriquez, A. (2025). A meta-analysis assessment of adaptive and transformative approaches to supply chain resilience. *Supply Chain Analytics*, 10, 100124. <https://doi.org/10.1016/j.sca.2025.100124>
- Anton, S. G., & Nucu, A. E. A. (2020). Enterprise risk management: A literature review and agenda for future research. *Journal of Risk and Financial Management*, 13(11), 281. <https://doi.org/10.3390/jrfm13110281>
- Chang, X., Song, Z., & Zhou, T. (2025). Geopolitical risk and global supply chain resilience. *Finance Research Letters*, 86, 108551. <https://doi.org/10.1016/j.frl.2025.108551>
- Chung, S. H., Wallace, S. W., & Wen, X. (2025). Data driven operational risk management. *Annals of Operations Research*, 348(2), 777–781. <https://doi.org/10.1007/s10479-025-06598-5>
- Cui, J., Pan, J., & Song, Z. (2025). Sourcing and supplying strategies under supply risk of critical components. *European Journal of Operational Research*, 327(1), 136–147. <https://doi.org/10.1016/j.ejor.2025.05.010>
- Dahmen, P. (2023). Organizational resilience as a key property of enterprise risk management in response to novel and severe crisis events. *Risk Management and Insurance Review*, 26(2), 203–245. <https://doi.org/10.1111/rmir.12245>
- Dong, F., Zhao, X., Mangla, S. K., & Song, M. (2025). Enhanced supply chain resilience under geopolitical risks: The role of artificial intelligence. *Transportation Research Part E: Logistics and Transportation Review*, 202, 104300. <https://doi.org/10.1016/j.tre.2025.104300>

- Gleißner, W., & Berger, T. B. (2024). Enterprise risk management: Improving embedded risk management and risk governance. *Risks*, 12(1), 20. <https://doi.org/10.3390/risks12010020>
- Hosseini Shekarabi, S. A., Kiani Mavi, R., & Romero Macau, F. (2025). Supply chain resilience: A critical review of risk mitigation, robust optimisation, and technological solutions and future research directions. *Global Journal of Flexible Systems Management*, 26, 681–735. <https://doi.org/10.1007/s40171-025-00458-8>
- Hou, D., Wu, Z., & Chen, Y. (2025). Climate risk exposure and corporate strategic dualism: Passive defensiveness and active integration. *Sustainability*, 17(13), 6040. <https://doi.org/10.3390/su17136040>
- Latsiou, A., & Lambrinoudakis, C. (2026). Cyber supply chain risk management: From threats to treatment. *International Journal of Information Security*, 25, Article 40. <https://doi.org/10.1007/s10207-025-01207-9>
- Lei, S., Chen, Y., & Xia, D. (2025). Does climate risk disclosure affect stock liquidity? *Research in International Business and Finance*, 80, 103130. <https://doi.org/10.1016/j.ribaf.2025.103130>
- Liu, Y., Xi, M., Zhou, Y., Feng, T., Fang, W., & Wang, W. (2025). Invisible threats: The impact of perceived political risk misalignment on firm's operational resilience. *Transportation Research Part E: Logistics and Transportation Review*, 200, 104186. <https://doi.org/10.1016/j.tre.2025.104186>
- López, C., Morales-Contreras, M. F., Langella, I. M., & Alonso-Monge, J. (2025). Modeling supply chain disruptions due to geopolitical reasons: A systematic literature review. *Transportation Research Part E: Logistics and Transportation Review*, 202, 104290. <https://doi.org/10.1016/j.tre.2025.104290>
- Malik, F. S., & Terzidis, O. (2026). Thriving in turbulence: Resilience and strategic adaptation in global business. *Review of Managerial Science*, 20, 2349–2394. <https://doi.org/10.1007/s11846-025-00940-8>
- McLemore, P., & Mihov, A. (2026). AI and operational losses: Evidence from U.S. bank holding companies. *The Review of Corporate Finance Studies*. Advance online publication. <https://doi.org/10.1093/rcfs/cfag003>
- Monazzam, A., & Crawford, J. (2024). The role of enterprise risk management in enabling organisational resilience: A case study of the Swedish mining industry. *Journal of Management Control*, 35(1), 59–108. <https://doi.org/10.1007/s00187-024-00370-9>
- Naseer, M. M., Guo, Y., & Zhu, X. (2025). The dynamics of corporate climate risk and market volatility: International evidence. *The North American Journal of Economics and Finance*, 78, 102435. <https://doi.org/10.1016/j.najef.2025.102435>
- Orwat, C., Bareis, J., Folberth, A., Jahnelt, J., & Wadephul, C. (2024). Normative challenges of risk regulation of artificial intelligence. *NanoEthics*, 18, Article 11. <https://doi.org/10.1007/s11569-024-00454-9>
- Paul, A., & Saha, S. C. (2025). A systematic literature review on flexible strategies and performance indicators for supply chain resilience. *Global Journal of Flexible Systems Management*, 26(Suppl. 1), 207–231. <https://doi.org/10.1007/s40171-024-00415-x>

- Qiu, Y., Chen, J., & Ding, Q. (2025). Corporate climate risk exposure and stock liquidity: New evidence based on heterogeneous environmental regulation. *Research in International Business and Finance*, 79, 103089. <https://doi.org/10.1016/j.ribaf.2025.103089>
- Rajendra, J. B., & Thuraisingam, A. S. (2026). The role of explainability and human intervention in AI decisions: Jurisdictional and regulatory aspects. *Information & Communications Technology Law*, 35(2), 152–183. <https://doi.org/10.1080/13600834.2025.2537514>
- Seid, E., Ilter, D., Blix, F., & Popov, O. (2025). Cyber supply chain resilience: Analyzing ISO, NIST, and NIS2 frameworks for mitigating third-party risks. *Procedia Computer Science*, 263, 591–599. <https://doi.org/10.1016/j.procs.2025.07.071>
- Szadeczky, T., & Bederna, Z. (2025). Risk, regulation, and governance: Evaluating artificial intelligence across diverse application scenarios. *Security Journal*, 38, Article 35. <https://doi.org/10.1057/s41284-025-00495-z>
- Taeihagh, A. (2025). Governance of generative AI. *Policy and Society*, 44(1), 1–22. <https://doi.org/10.1093/polsoc/puaf001>
- Ulnicane, I. (2025). Governance fix? Power and politics in controversies about governing generative AI. *Policy and Society*, 44(1), 70–84. <https://doi.org/10.1093/polsoc/puae022>
- Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the draft EU Artificial Intelligence Act: Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International*, 22(4), 97–112. <https://doi.org/10.9785/cr-2021-220402>
- Wang, M., & Wang, X. (2025). Geopolitical risk and corporate maturity mismatch. *Journal of Financial Stability*, 78, 101408. <https://doi.org/10.1016/j.jfs.2025.101408>
- Wang, M., Yu, X., Feng, S., & Xu, C. (2025). The application of artificial intelligence in corporate climate risk: Information disclosure, information advantage, and information prediction. *Journal of Cleaner Production*, 534, 147040. <https://doi.org/10.1016/j.jclepro.2025.147040>
- Xiong, D., & Sun, Y. (2025). The rising cost of turmoil: Geopolitical crises and supply chain risk. *Economics Letters*, 255, 112582. <https://doi.org/10.1016/j.econlet.2025.112582>
- Yu, J., Fang, Y., Bai, Y., & Chen, F. (2025). Building resilience amidst geopolitical tensions: The case of U.S. MNE subsidiaries in China. *Journal of International Management*, 31(4), 101260. <https://doi.org/10.1016/j.intman.2025.101260>
- Yusof, M. S. (2025a). Technology adoption in small and medium enterprises and its impact on business growth, innovation, and digital sustainability. *International Journal of Advanced Research in Economics and Finance*, 7(3), 84–100. <https://doi.org/10.55057/ijaref.2025.7.3.7>
- Yusof, M. S. (2025b). The influence of digital adoption on the growth and resilience of rural agro-food entrepreneurs. *International Journal of Business and Technology Management*, 7(6), 316–334. <https://doi.org/10.55057/ijbtm.2025.7.6.27>
- Zhou, G., & Zhao, C. (2026). An explainable machine learning framework linking ESG performance and supply chain resilience prediction: Evidence from Chinese listed companies. *Humanities and Social Sciences Communications*. <https://doi.org/10.1057/s41599-026-0843>