Risk and Optimization of Digital Transformation in Supply Chain: A Literature Review

Jieyu Shi *

Department of Industrial Engineering, Sichuan University, Chengdu, China

* Corresponding Author Email: 2022141520106@stu.scu.edu.cn

Abstract. This study investigates the risks and optimization strategies associated with the digital transformation of supply chains through a systematic literature review combined with case-based analysis. Drawing on both academic research and enterprise practices, the study identifies three primary risk dimensions-technological, data-related, and external environmental-and examines their dynamic interrelations. The findings reveal that while digital transformation enhances visibility, efficiency, and competitiveness, it simultaneously amplifies systemic vulnerabilities due to increased interconnectivity and data dependency. Based on a synthesis of existing literature and empirical case evidence from JD, Walmart, and Alibaba, the study proposes a Technology-Data-Environment (TDE) Framework to conceptualize the cascading mechanisms of digital supply chain risks. Furthermore, three optimization pathways-technological reinforcement, data governance enhancement, and resilience-oriented management-are proposed to mitigate multidimensional risks and strengthen adaptive capacity. The study contributes to the theoretical integration of digital transformation and supply chain risk management and provides actionable insights for practitioners pursuing sustainable digitalization.

Keywords: Digital transformation, supply chain risk, resilience, data governance, technological innovation, risk management.

1. Introduction

In an era of accelerating digitalization, supply chains are undergoing a profound structural transformation driven by technologies such as artificial intelligence, big data analytics, cloud computing, and blockchain. This digital transformation promises enhanced operational efficiency, agility, and market responsiveness. However, it also introduces new sources of systemic risk due to increased technological interdependence, data complexity, and exposure to external shocks.

While prior research has emphasized the performance benefits of digital transformation, limited attention has been paid to the accompanying multidimensional risks and their cascading mechanisms. Moreover, few studies have integrated theoretical perspectives with empirical evidence from enterprise practice. To address this gap, this study adopts a systematic literature review (SLR) combined with case-based analysis to explore (1) the mechanisms through which digital transformation generates technological, data-related, and environmental risks, and (2) the strategies firms can adopt to mitigate these risks and enhance resilience.

This study makes two primary contributions. First, it develops the Technology–Data–Environment (TDE) Framework, offering a holistic perspective on the interdependencies of digital risks in supply chains. Second, it proposes a set of integrated optimization strategies that bridge theory and practice, providing both conceptual advancement and managerial guidance for sustainable digital transformation.

2. Literature Review

A literature review is a systematic synthesis and critical evaluation of existing research in a specific field. Its main purpose is to describe the current state of knowledge, identify existing research gaps, and lay a conceptual foundation for future research. In this study, the focus of the review is on the digital transformation of the supply chain and its related risk mechanisms, with particular attention to the interrelated structure of digital transformation, supply chain risk, and resilience.

Digital transformation in supply chain management (SCM) refers to the strategic integration of digital technologies such as intelligent systems, big data analytics, and cloud computing into supply chain processes to achieve operational optimization and structural restructuring. Digital transformation has become a strategy to enhance resilience. It not only involves the adoption of tools, but also the restructuring of processes, resource allocation, and coordination (Verhoef et al., 2021), as emphasized by Boldrini et al. (2025) in their macro fintech framework. Digital capabilities have improved the agility of companies in data usage, operations, and organizational design (Merin Rodriguez et al., 2024; Sun et al., 2025) [4]. On the contrary, supply chain risks include a range of internal and external uncertainties that may jeopardize operational stability during the transition period. The specific types of risks include cascading failures, where local interruptions propagate between interdependent nodes, leading to system failures [3], and data silos, which are caused by insufficient standardization and hinder effective information exchange between supply chain partners [5]. In contrast, supply chain resilience refers to the system's ability to absorb shocks, adapt to disturbances, and maintain functionality under fluctuating conditions.

2.1. Digital Transformation and Operational Efficiency

Existing research consistently indicates that digital transformation has become a key driving force for improving supply chain management, especially in the face of increasing pressure from global competition, uncertainty, and industrial restructuring. Digital transformation, as a new factor of production, not only reshapes traditional business models, but also plays a crucial role in improving supply chain efficiency and resilience. Digital transformation has not only changed the internal operational model of enterprises, but also had a profound impact on their external supply chain relationships. By introducing advanced information technologies such as big data, artificial intelligence, and the Internet of Things, enterprises can achieve intelligent management of their supply chain, thereby improving its transparency, flexibility, and responsiveness [8]. For example, JD's intelligent logistics infrastructure, Wal Mart's analysis driven inventory management, and Alibaba's empirical evidence of integrating e-commerce with cloud-based logistics show that technology empowerment can significantly improve coordination, shorten delivery cycles, and optimize resource allocation. Overall, these findings emphasize that digital transformation is a key driving factor for operational excellence in modern supply chains.

2.2. Risks in the Digital Transformation Process

Although digital transformation has introduced new sources of competitive advantage, it has also increased exposure to technological, informational, and environmental vulnerabilities.

Technical risks arise from system integration complexity, interoperability challenges, and automation failures. Zhu et al. (2025) discovered a "cascading failure" effect, where local technical interruptions may trigger full chain failures [3]. Real world cases such as logistics delays caused by mismatched system interfaces on JD.com and order processing errors caused by system architecture conflicts on Alibaba demonstrate the fragility of highly digital networks.

The risks associated with data stem from the explosion and heterogeneity of data exchange. Esmaeeli et al. (2024) emphasize that inadequate security protocols and unclear data ownership often lead to data breaches and inefficiencies. The continued existence of 'data silos' exacerbates these challenges. Wal Mart's data leakage incident was attributed to third-party vulnerabilities, reflecting the operational consequences of weak data governance.

External environmental risks include external shocks such as geopolitical conflicts, natural disasters, epidemics, and policy shifts. Ding et al. (2025) and Boldrini et al. (2024) demonstrated that geopolitical crises and trade barriers can disrupt global supply networks [6], while public health emergencies and natural disasters can disrupt logistics continuity and production capacity (Ye et al., 2024; Butt, 2021) [7]. Therefore, the increasing interdependence of global supply chains has increased the risk of systemic exposure to such external shocks.

2.3. Risk Management and Supply Chain Resilience

To mitigate these vulnerabilities, previous studies have emphasized the necessity of incorporating risk management and resilience building mechanisms into digital supply chain strategies (Manuj&Mintzer, 2008; Chaudhuri et al., 2018); Piprani et al., 2022) [2]. Technological innovation has further strengthened these capabilities. Sabarmati (2025) emphasizes the potential of blockchain in improving data traceability and transaction security, and blockchain technology (BT) has become a transformative solution to enhance the effectiveness, security, and transparency of supply chain intelligence. Traditional supply chain management (SCM) systems often suffer from issues such as data silos, lack of real-time visibility, fraudulent activities, and inefficient tracking and traceability. The decentralization and irreversible ledger of blockchain provide a solid foundation for addressing these issues; It promotes trust, security, and real-time data sharing among all stakeholders. Liu et al. (2024) emphasized the role of digital transparency in enhancing adaptive response and resilience [2]. Therefore, the literature unanimously agrees that combining digital innovation with resilience engineering is a strategic priority for sustainable supply chain performance in the digital age.

3. Research Methodology

This study adopts a systematic literature review (SLR) in conjunction with case-based analysis to investigate the multidimensional risks and optimization strategies associated with supply chain digital transformation. The methodology integrates theoretical synthesis with empirical validation, following four key stages: literature retrieval, screening, analysis, and case verification.

3.1. Literature Retrieval

A comprehensive search was conducted across major academic databases and industry sources using keywords such as “digital transformation of supply chain,” “supply chain risk,” “technological risk,” “data risk,” “external environmental risk,” and “optimization strategy.” The dataset encompasses both academic contributions (e.g., Choi et al., 2019; Ivanov & Dolgui, 2020) and industry case materials derived from enterprises such as JD, Walmart, and Alibaba. This dual-source approach ensures a balanced synthesis of theoretical insights and real-world evidence.

3.2. Literature Screening

A two-stage screening process was employed to ensure the rigor and relevance of selected materials:

Stage 1 (Preliminary Screening): Titles and abstracts were reviewed to eliminate studies not directly addressing digital transformation risks or optimization mechanisms.

Stage 2 (Full-Text Evaluation): Articles lacking methodological soundness, theoretical contribution, or empirical substantiation were excluded.

Ultimately, seven core academic references and multiple enterprise case studies were retained as the empirical and conceptual foundation for this study.

3.3. Literature Analysis

The selected literature was systematically classified into three analytical dimensions—technological, data-related, and external environmental risks. Within each category, the study extracted the key theoretical propositions, methodological frameworks, and empirical findings, subsequently comparing their points of convergence and divergence. Corporate case materials—such as JD’s logistics system malfunction and Walmart’s data breach—were used to validate these theoretical constructs, ensuring the alignment between scholarly insights and practical realities.

3.4. Case-Based Verification

To substantiate the theoretical framework, three representative enterprises—JD, Walmart, and Alibaba—were selected for case verification. Each case was analyzed in terms of digital technology

deployment, encountered risk types, and adopted mitigation strategies. For instance, JD's logistics system failure illustrates integration complexity and interoperability risks, whereas Walmart's data leakage underscores the consequences of insufficient data security mechanisms. Through these cases, the study empirically validates the multidimensional nature of digital transformation risks and assesses the practical feasibility of proposed optimization strategies.

4. Results and analysis

4.1. Multidimensional Risk Mechanisms in Supply Chain Digital Transformation

The systematic review and case analysis reveal that risks in supply chain digital transformation are multidimensional and interdependent, encompassing technological, data-related, and external environmental domains. These risk dimensions do not exist in isolation but often interact, forming a cascading structure that amplifies system vulnerability.

4.1.1. Technological risk mechanism

Technical risks arise from the complexity of system integration, technical incompatibility, and automation failures. The case of JD Logistics system failure illustrates how the coupling of multiple digital subsystems can create unexpected interdependencies, leading to cascading interruptions. Cascade failure is a common risk propagation mechanism in complex systems. It refers to the phenomenon where a node fails due to interference or impact, and its original functions or loads are redistributed to other nodes. If these nodes cannot bear the additional burden, they may also fail continuously, ultimately triggering a chain reaction and leading to large-scale system crashes [9]. Similarly, Alibaba's system conflicts during peak trading periods demonstrate the fragility of complex digital architectures under high-capacity pressure.

4.1.2. Data risk mechanism

Data-related risks stem from both structural and managerial deficiencies in data governance. Empirical evidence indicates that insufficient data standardization results in fragmented information silos, while weak security protocols expose firms to cyberattacks and privacy breaches. Walmart's data leakage incident underscores the vulnerability of third-party platforms in interconnected ecosystems. These findings echo Esmaeeli et al. (2024), who emphasize that the lack of full-process data protection mechanisms remains a fundamental bottleneck in achieving secure and transparent supply chains [5].

4.1.3. External environmental risk mechanism

External risks, such as geopolitical disruptions, pandemics, and policy changes, further exacerbate supply chain instability. The COVID-19 pandemic and regional trade tensions have exposed the fragility of global supply interdependencies. Consistent with Ding et al. (2025) and Ye et al. (2024), this study confirms that digitalized supply chains, while enhancing visibility and responsiveness, remain susceptible to large-scale external shocks that transcend technological control [7].

Collectively, these three risk dimensions interact through cascade coupling effects, forming a multidimensional risk network. For instance, a technological failure (e.g., system outage) can lead to data disruption, which subsequently magnifies external exposure by impairing decision-making speed and accuracy. This dynamic interaction underscores the necessity of developing a holistic risk governance framework that integrates digital, organizational, and environmental resilience.

4.2. Optimization Strategies for Digital Supply Chain Risk Mitigation

Based on the cross-analysis of literature and enterprise cases, this study identifies three major optimization pathways—technological reinforcement, data governance enhancement, and resilience-oriented management—that collectively mitigate the multidimensional risks identified above.

4.2.1. Technological reinforcement and system redundancy

Enterprises should prioritize modular architecture design and technological redundancy to prevent systemic collapse caused by single-node failures. As evidenced by JD's infrastructure upgrades, adopting layered architectures and fault-tolerant systems can reduce the propagation of technical shocks. The establishment of digital twin systems further allows firms to simulate disruptions and preemptively identify potential vulnerabilities before implementation.

4.2.2. Data governance enhancement and secure interoperability

Effective digital transformation necessitates comprehensive data governance mechanisms that balance transparency with security. The adoption of standardized data protocols, end-to-end encryption, and blockchain-enabled traceability enhances both data integrity and accountability. As demonstrated in Sabarmati (2025), blockchain integration strengthens inter-firm trust by providing immutable transaction records, thereby mitigating risks associated with data manipulation and unauthorized access [1].

4.2.3. Resilience-oriented management and adaptive capability

The cultivation of resilience extends beyond technological solutions to encompass organizational flexibility and strategic adaptability. Firms such as Alibaba have adopted multi-sourcing strategies, real-time monitoring systems, and AI-driven predictive analytics to maintain operational continuity amid external shocks. This finding resonates with Manuj and Mentzer (2008), who argue that resilience depends on the interplay between structural robustness, flexibility, and rapid recovery capacity. The empirical evidence suggests that enterprises capable of dynamically reallocating resources and reconfiguring operations exhibit superior post-disruption recovery performance [2].

4.3. Theoretical and Managerial Implications

From a theoretical standpoint, this study contributes to the literature by proposing a "Technology–Data–Environment (TDE)" risk interaction framework, which elucidates the cascading mechanisms linking digital infrastructure, data flows, and external uncertainties. This framework advances existing SCM theories by integrating digital transformation risks into a systemic and adaptive perspective, extending beyond traditional static models of operational risk.

From a managerial perspective, the findings emphasize that digital transformation should not be viewed merely as a technological upgrade but as a strategic reconfiguration of risk governance. Enterprises are advised to integrate digital investment decisions with resilience management, establishing cross-functional digital risk committees, and adopting predictive analytics to enhance real-time response capabilities.

4.4. Discussion Summary

In sum, digital transformation introduces both opportunities and vulnerabilities into the supply chain ecosystem. While digital technologies enhance visibility, efficiency, and coordination, they simultaneously expose firms to complex, multi-layered risks. The interaction among technological, data, and external risk factors constitutes a dynamic network that requires proactive, system-level management. Therefore, the key to sustainable digital transformation lies in balancing efficiency gains with resilience enhancement, ensuring that technological innovation is accompanied by adaptive risk governance and robust organizational learning mechanisms.

5. Conclusion

This study systematically examined the risks and optimization strategies inherent in the digital transformation of supply chains by integrating a systematic literature review with case-based empirical analysis. Drawing upon both academic research and real-world enterprise practices, the findings reveal that digital transformation, while offering substantial operational benefits,

simultaneously generates complex and interdependent risks across technological, data-related, and external environmental dimensions.

Specifically, technological risks arise from the integration complexity of digital systems and potential cascade failures across interconnected nodes; data risks stem from insufficient standardization, inadequate security mechanisms, and fragmented data ownership; and external risks are amplified by global uncertainties such as geopolitical instability, natural disasters, and public health crises. These three risk dimensions are not isolated but dynamically interlinked, forming a cascading network of vulnerabilities that can propagate disruptions throughout the entire supply chain system.

To address these challenges, this study proposes three key optimization pathways: (1) technological reinforcement, emphasizing modular architecture and system redundancy; (2) data governance enhancement, focusing on standardized data management and blockchain-based traceability; and (3) resilience-oriented management, prioritizing adaptive capacity and organizational flexibility. Collectively, these strategies enable firms to transition from reactive risk mitigation to proactive resilience building.

By conceptualizing the interrelations among these risk domains, the study introduces the Technology–Data–Environment (TDE) Framework, which captures the multidimensional and interactive nature of digital supply chain risks. This framework underscores the necessity of integrating technological innovation with systemic risk governance to achieve sustainable digital transformation.

References

[1] Simarmata, J. E. (2025). How blockchain technology manages supply chain risk. In N. A. Rahman et al. (Eds.), Supply Chain in Humanitarian Operations (pp. 85 – 99). Springer Nature Singapore. https://doi.org/10.1007/978 - 981 - 96 - 4426 - 1_8.

[2] Liu, Y., Du, J., Kang, T., & Kang, M. (2024). Establishing supply chain transparency and its impact on supply chain risk management and resilience. Operations Management Research, *17*, 1157 – 1171. https://doi.org/10.1007/s12063 - 024 - 00499 - 9.

[3] Zhu, X.-X., Zhu, J., Regan, D., & Wen, Z.-M. (2025). Exploring cascading failures in supply chain risk management: A systematic review, 2013 – 2024. Journal of Safety Science and Resilience, *100234*. https://doi.org/10.1016/j.jnlssr.2025.100234.

[4] Chen, W., Wang, J., & Wang, S. (2025). Economic uncertainty, digital transformation, and firm supply chain disruption risk. *Economics Letters*, *255*, 112516. https://doi.org/10.1016/j.ecolet.2025.112516.

[5] Esmaeeli, Z., Mollaverdi, N., & Safarzadeh, S. (2024). A game theoretic approach for green supply chain management in a big data environment considering cost-sharing models. Expert Systems with Applications, *257*, 124989. https://doi.org/10.1016/j.eswa.2024.124989.

[6] Xiong, D., & Sun, Y. (2025). The rising cost of turmoil: Geopolitical crises and supply chain risk. Economics Letters, *247*, 112582. https://doi.org/10.1016/j.econlet.2025.112582.

[7] Ye, Y., Wang, H., Tian, K., & Li, M. (2024). Supply chain risks and the cost of debt: Evidence from the COVID-19 pandemic. Research in International Business and Finance, *70*, 102399. https://doi.org/10.1016/j.ribaf.2024.102399.

[8] Fan, Y., Chen, X., Guo, X., & Bai, K. (2025). How does digital transformation improve supply chain efficiency? Evidence from A-share listed companies in China. Finance Research Letters, 86, 108549. https://doi.org/10.1016/j.frl.2025.108549.

[9] Kumar, P. R., Mohammad, G. B., Narsimhulu, P., Narasappa, D., Maguluri, L. P., Singh, S., & Selvarajan, S. (2025). Computer modeling approaches for blockchain-driven supply chain intelligence: A review on enhancing transparency, security, and efficiency. Computer Modeling in Engineering & Sciences, 144 (3), 2779 – 2812.https://doi.org/10.32604/cmes.2025.066365.

[10] Fu, X., Tian, M., Liu, X., Wu, S., & Peng, R. (2025). Cascading failure resilience of dual-layer supply chain networks under enterprise competition with incomplete information. Reliability Engineering and System Safety, *266*, 111735. https://doi.org/10.1016/j.ress.2025.111735.