



Domino Effect of Risk Exploring Cascading Threats Across Interconnected Business Systems

Ahmad Fauzi Ahmad Zaini^{1*}, Airuddin Ahmad²

^{1,2} Institute of Graduate Studies, Universiti Poly-Tech Malaysia, Malaysia

CORRESPONDING AUTHOR

Ahmad Fauzi Ahmad Zaini
Email: ahmadfauzi@uptm.edu.my
ORCID: 0000-0000-0000-0000

ARTICLE HISTORY

Received	Revised	Accepted	Published
13 June 2026	23 July 2026	17 August 2026	30 September 2026

ABSTRACT

Risk becomes far more consequential when a disruption is able to travel, interact, and multiply across the systems that support modern business. This article examines the cascading nature of contemporary threats by exploring how failures originating in suppliers, infrastructure, digital platforms, logistics networks, and other critical nodes can propagate through interconnected organisational relationships and generate second and third order consequences. The analysis shows that systemic vulnerability is shaped not only by the severity of the initiating event, but also by hidden dependencies, structural concentration, behavioural responses, digital interdependence, information asymmetry, and the way recovery actions redistribute pressure across the network. Particular attention is given to the limitations of conventional risk registers that isolate individual threats while overlooking the pathways through which disruption can spread. The article therefore advances a broader interpretation of resilience based on dependency intelligence, selective structural redundancy, coordinated response mechanisms, digital continuity, and intelligent system reconfiguration. Strategic recommendations further emphasise dynamic network mapping, redesign of critical connections, cross organisational response protocols, cyber physical risk governance, and systemic recovery quality as essential mechanisms for containing cascading threats before they develop into wider instability. The central argument is that resilience should no longer be judged solely by an organisation's ability to survive the first disruption, but by its capacity to prevent that disruption from becoming the trigger for subsequent failures across the wider business system.

Keywords: Cascading, Resilience, Interdependence, Propagation, Systemic

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.xxxx/ijbma.xxxxx>

COPYRIGHT & OPEN ACCESS

Copyright © 20XX 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

A disruption rarely remains confined to the place where it begins. Within increasingly interconnected business environments, the failure of a supplier, technology platform, logistics hub, financial institution, or operational process can transmit pressure across multiple organisational boundaries and create consequences far beyond the original point of disturbance. This phenomenon has become increasingly important as firms depend on dense networks of suppliers, customers, digital systems, transportation infrastructure, financial relationships, and strategic partners. Namdar et al., (2024) explain that cascading disruptions emerge when an initial disturbance propagates through connected firms and suppliers, although the magnitude and severity of propagation are strongly influenced by network structure. Evidence from intertwined supply networks similarly demonstrates that disruptions can move across shared suppliers and interconnected industries, creating ripple effects that cannot be adequately understood through isolated firm level analysis (Ivanov, 2023). Echefaj et al., (2024) further show that interconnections among automotive, healthcare, and electronics supply chains can alter both disruption impacts and recovery patterns, demonstrating that resilience within one system may depend substantially on conditions elsewhere in the broader network. Risk management must therefore move beyond identifying individual threats towards understanding how relationships between organisations, technologies, infrastructure, and resources create pathways through which disturbances can travel, interact, and intensify. Risk governance also depends on managerial judgement because perceptions of uncertainty shape how decision makers interpret emerging threats and select proportionate responses, a relationship emphasised by Yusof and Razali (2020).

What makes cascading risk particularly difficult to manage is that the eventual damage may bear little resemblance to the event that initiated it. A relatively localised disruption can generate successive operational consequences as affected organisations redistribute workloads, seek alternative suppliers, redirect inventories, modify production schedules, or compete for already constrained resources. Recent empirical evidence demonstrates that interacting risks can create a domino effect that produces supply instability, operational difficulties, innovation inefficiency, and deterioration in market performance (Binh et al., 2025). Zeng et al., (2025) similarly demonstrate that increasing interdependence between physical execution systems and information decision systems can heighten supply chain fragility, particularly when critical functions are concentrated within focal organisations. From a broader systems perspective, Huang et al., (2025) show that network effects and risk co-contagion can generate cascading failures that complicate the accurate assessment of systemic financial risk. These findings expose an important limitation of conventional risk registers that evaluate threats primarily according to their individual probability and impact. Such approaches may identify the first disruption while overlooking second and third order consequences created through interdependency. Effective risk analysis consequently requires attention not only to what can fail, but also to what becomes vulnerable when that failure changes the operating conditions of connected components. Operational interdependence is equally visible in warehousing and supply chain coordination, where strategic management choices can influence performance across connected activities (Abdullah et al., 2020).

Network architecture plays a decisive role in determining whether an initial disturbance is contained, amplified, or transformed into a system wide threat. Namdar et al., (2024) demonstrate that highly modular supply networks can restrict the overall spread of cascading disruptions because fewer connections exist between modules, yet dense connectivity within individual modules can

simultaneously intensify disruption severity among closely connected suppliers. Cao et al., (2025) reach a related conclusion in their analysis of the global container shipping network, showing that high interconnectedness creates resilience challenges when extreme events trigger cascading failures and force cargo loads to be redistributed across alternative ports. Further evidence from complex multi-tier supply chains indicates that resilience depends substantially on the interplay between network tiers and connections rather than on the condition of individual organisations alone. These findings reveal a fundamental paradox within contemporary business systems. Connectivity creates efficiency by facilitating coordination, specialisation, resource sharing, information exchange, and global market access, but the same connectivity can create transmission channels through which disruption travels. Organisations can therefore become exposed to risks originating from firms or infrastructure they do not directly control and may not even recognise as strategically significant. Understanding network structure becomes essential because resilience depends increasingly on where dependencies are concentrated and how alternative pathways can function when critical connections fail. Earlier cross-functional coordination can prevent a contained disturbance from becoming a network-wide continuity failure.

Another complication arises from the dynamic character of cascading threats. Business networks continuously change as organisations enter and exit markets, suppliers are replaced, capacities fluctuate, technologies evolve, and commercial relationships are reconfigured. Static risk assessments can therefore become unreliable when they assume that dependencies remain stable throughout a disruption. Shi et al., (2026) demonstrate that supply chain resilience is influenced not only by network topology but also by the evolving interaction between node capacities, load distributions, recovery potential, and changes in network relationships over time. Fu et al., (2026a) further show that enterprise competition and incomplete information influence how cascading failures propagate because organisations respond to disruption through competitive resource redistribution and the selection of substitute partners. Hu et al., (2026) similarly argue that contemporary supply chain risk analysis must account for heterogeneous failure characteristics and adaptive recovery strategies rather than relying exclusively on simplified single failure assumptions. Cascading risk should consequently be understood as an evolving process rather than a predetermined sequence of failures. Organisational responses can redirect disruption, transfer pressure to alternative nodes, create unexpected bottlenecks, or generate new vulnerabilities. Risk governance must therefore incorporate temporal dynamics, behavioural responses, information quality, and recovery capacity when evaluating how an apparently manageable disturbance might develop into a wider systemic problem. Global shipping cases also illustrate how innovation and network dependence can coexist, making continuity planning important when transport connections become concentrated or disrupted (Cao et al., 2025).

Recognising the domino effect of risk ultimately requires a shift from protecting individual organisational components towards governing resilience across interconnected systems. The objective is not to eliminate every possible disruption, which is increasingly unrealistic, but to prevent local failures from acquiring sufficient momentum to destabilise critical business functions. Recent research demonstrates that collaborative coordination of shared inventories and repurposed capacities can mitigate ripple effects within intertwined supply networks (Ivanov, 2023). Resilience can also be strengthened through appropriate redundancy and load redistribution strategies that prevent excessive pressure from accumulating at critical nodes following disruption. Fu et al., (2026a) additionally find that greater information transparency can enhance supply chain resilience against cascading failures, highlighting the importance of visibility when organisations must rapidly

identify substitute resources and changing network conditions. These developments establish the need for a more systemic interpretation of contemporary business risk. Intermodal logistics further demonstrates that resilience depends on coordination across transport modes, partners, and information flows rather than on isolated operational efficiency (Roshani et al., 2024). This temporal perspective helps managers choose redundancy, substitution, and escalation measures according to how the network is actually changing. Resilience therefore becomes a continuously renewed capability shaped by changing technologies, relationships, capacities, and external conditions. Managers should therefore trace dependencies as transmission pathways, not record them as isolated operational exposures. This orientation strengthens preparedness across connected business relationships.

2. LITERATURE REVIEW

The intellectual foundation for understanding cascading business threats has shifted considerably as organisations have become embedded within increasingly dense networks of operational, technological, financial, and supply relationships. Contemporary research no longer treats resilience solely as the capacity of an individual organisation to withstand disruption, but increasingly examines how failures propagate through connections among firms and infrastructure. Fu et al., (2026b) describe cascading failure as a chain reaction in which failures among a limited number of nodes can progressively impair an entire supply chain system, while Hu et al., (2026) emphasise that modern network complexity and interdependence substantially increase exposure to such propagation. Research has consequently expanded from conventional disruption analysis towards network topology, propagation mechanisms, recovery dynamics, information flows, and adaptive resilience. Zhou et al., (2026) further demonstrate that risk propagation interacts with risk awareness across interconnected resource and information networks, indicating that organisational behaviour can influence the trajectory of disruption rather than merely respond to its consequences. This literature provides an important basis for explaining the domino effect of risk because it establishes that the severity of disruption depends not only on the initiating event, but also on network structure, dependency concentration, information quality, organisational heterogeneity, and the capacity of connected actors to absorb and redistribute pressure.

2.1 Cascading Risk Dynamics Shaping Complex Threat Propagation Patterns

A seemingly manageable failure can acquire systemic significance once its consequences begin crossing organisational boundaries. Cascading risk differs from an isolated operational disruption because the initial disturbance changes conditions elsewhere in the network, potentially overloading connected organisations, interrupting resource flows, reducing capacity, or generating additional failures. Fu et al., (2026b) demonstrate through a systematic review that cascading failures have become a major concern for supply chain stability because the failure of a relatively small number of nodes can trigger extensive chain reactions throughout the system. Hu et al., (2026) similarly argue that risks affecting particular firms can propagate through network relationships and potentially destabilise wider supply structures, especially when firms differ in capacity and vulnerability. Cao et al., (2025) provide sectoral evidence from the global container shipping network, demonstrating how extreme events can initiate cascading failures within highly interconnected transportation structures and how subsequent load redistribution influences resilience. Collectively, these studies demonstrate that risk propagation should be understood as a dynamic transmission process rather than a collection of independent failures. The eventual impact depends on where disruption originates, how operational loads are transferred, which nodes receive

additional pressure, and whether alternative connections possess sufficient capacity to absorb the resulting disturbance. Cascading risk therefore changes the analytical question from identifying what may fail towards understanding how an initial failure can alter the vulnerability of everything connected to it.

Propagation becomes considerably more complex when several mechanisms operate simultaneously. Zeng et al., (2025) demonstrate that cyber physical supply chain structures combine physical execution and information decision layers, meaning disruption can travel through different but interconnected dimensions of the same system. Zhou et al., (2026) extend this reasoning through a dual layer model connecting the propagation of operational risk with the dissemination of risk awareness, revealing that firms' willingness and ability to resist disruption can alter network resilience. Research on cyber physical supply chains similarly shows that real systems can experience multiple failure modes rather than a single uniform mechanism, requiring resilience strategies capable of addressing different forms of cascading behaviour. Fu et al., (2026b) identify hybrid failure mechanisms and multilevel propagation patterns as important directions for advancing cascading failure research, reinforcing the inadequacy of models that assume a single transmission pathway. These findings provide a more sophisticated interpretation of the domino effect. One disruption does not necessarily generate another through a simple sequential pathway. It may simultaneously affect material availability, information quality, operational capacity, transportation flows, financial conditions, and organisational decision making. The resulting cascade can therefore accelerate, weaken, redirect, or combine with other disturbances as it travels. Effective analysis requires attention to these interacting transmission mechanisms because the visible disruption may represent only one manifestation of a much broader systemic process.

2.2 Network Interdependence Structures Driving Systemic Business Vulnerability Patterns

Connectivity creates efficiency, but every connection can also become a pathway through which disruption travels. Modern supply networks depend on extensive relationships among suppliers, manufacturers, logistics providers, distributors, technology platforms, financial institutions, and customers, creating structures in which organisational performance is increasingly dependent on actors beyond direct managerial control. Roshani et al., (2024) show that resilient supply chain network design requires deliberate consideration of disruption locations and mitigation strategies because network configuration fundamentally shapes vulnerability and recovery possibilities. Santos et al., (2025) similarly emphasise that disruption affecting a single supplier can create cascading consequences throughout the supply chain, reinforcing the importance of examining supplier related risk within the broader architecture of interconnected operations. Cao et al., (2025) demonstrate this structural vulnerability in global container shipping, where extensive interconnectedness increases exposure to cascading failures when extreme events disrupt strategically important ports. Such evidence challenges the assumption that more connections automatically create greater resilience. Additional relationships can provide alternative sourcing or transportation pathways, yet they can also increase the number of channels through which disturbance can propagate. The strategic value of connectivity therefore depends on the configuration, capacity, substitutability, and concentration of those relationships rather than connectivity alone. Digital warehouse systems can support resilience through improved information visibility and coordination, although their value depends on how effectively technology is integrated with wider supply chain processes (Yusof et al., 2025).

Critical nodes deserve particular attention because their structural importance can make them disproportionately influential during disruption. Zeng et al., (2025) find that increasing centralisation within supply chains can concentrate critical decision and operational functions among focal firms, improving coordination under normal conditions while simultaneously creating dependency and fragility. Research examining lithium supply chains provides a comparable perspective, showing that systemic risks propagate across life cycle stages and national boundaries through multilayer interconnections that cannot be adequately captured through static or single layer analysis. Shi et al., (2026) further demonstrate that network resilience depends not only on topology but also on evolving node capacities, operational loads, relationship turnover, and recovery potential. These findings reveal why highly connected organisations can become both stabilising anchors and systemic vulnerabilities. A focal organisation with substantial capacity may absorb disruption during normal disturbances, yet its failure can simultaneously affect numerous dependent actors. Conversely, highly decentralised structures may reduce concentration risk while increasing coordination complexity. Network resilience therefore requires a balance between efficiency, redundancy, flexibility, and dependency diversification. Understanding this balance is essential for cascading risk analysis because the location and structural importance of a failed node may be more consequential than the apparent magnitude of the original disruption itself. Smart warehouse technologies also create continuity considerations because system maintenance and security weaknesses can transmit operational consequences beyond a single facility (Yusof et al., 2025).

2.3 Risk Information Dynamics Shaping Organisational Response Behaviour Patterns

Information can either interrupt a cascade or become part of the mechanism that intensifies it. Organisations rarely possess complete visibility across complex business networks, particularly beyond immediate suppliers and customers, creating delays between the emergence of disruption and recognition of its wider implications. Zhou et al., (2026) demonstrate that risk information sharing interacts directly with operational risk propagation, and that strengthening organisational risk awareness can raise transmission thresholds while improving recovery capability. Fu et al., (2026a) add another dimension by examining enterprise competition under incomplete information. Their findings show that resource redistribution following failure is influenced by competitive and cooperative behaviour rather than occurring uniformly across neighbouring firms. This insight is particularly important because organisations responding rationally to their own interests may unintentionally increase systemic pressure elsewhere. A firm securing alternative capacity after a disruption, for example, may protect its own operations while reducing the resources available to other affected organisations. Information asymmetry can further distort these responses because decision makers may act before understanding the complete network consequences. Cascading risk therefore involves behavioural as well as structural dynamics. Visibility, communication speed, information credibility, organisational incentives, and competitive behaviour influence whether early warning signals produce coordinated containment or fragmented responses that redistribute vulnerability throughout the network. Digital capability can improve organisational growth and adaptability, but greater technological dependence also increases the importance of continuity controls and responsible technology management (Yusof, 2025a).

Time introduces another layer of complexity because the network confronting a disruption may not remain structurally identical throughout the recovery process. Shi et al., (2026) argue that static resilience assessments overlook important changes involving firm entry and exit, relationship turnover, operational transitions, and recovery dynamics. Their temporal supply chain network

model demonstrates that resilience emerges from the evolving interaction between network structure and recovery potential rather than from topology alone. Hu et al., (2026) similarly criticise approaches that treat recovery as a discrete intervention and instead propose adaptive strategies across changing operational states. Stentoft and Mikkelsen (2024) approach resilience from a process perspective, reinforcing the importance of treating resilience development as an organised sequence of activities rather than a single organisational attribute. These perspectives substantially deepen understanding of cascading threats. A supplier considered noncritical under normal conditions may become indispensable after another supplier fails. An alternative logistics route may become overloaded as multiple organisations redirect shipments simultaneously. A temporary recovery decision may therefore create a new concentration of dependency that did not exist before the disruption. Risk assessment must consequently examine not only existing connections but also how those connections are likely to change as organisations adapt. Cascading threats evolve through the interaction between disruption and response, making temporal analysis indispensable to realistic resilience planning. The resulting evidence can guide selective buffers and alternative pathways without treating every connection as equally critical.

2.4 Digital Interdependence Creating Cyber Physical Cascading Threat Pathways

Business connectivity now extends far beyond physical supply relationships. Enterprise resource planning systems, cloud platforms, industrial automation, digital marketplaces, logistics technologies, connected devices, and shared information infrastructures have created cyber physical dependencies in which operational continuity increasingly depends on the uninterrupted interaction between digital and physical systems. Zeng et al., (2025) demonstrate that deeper coupling between physical execution and information decision layers can significantly increase supply chain fragility, particularly when critical functions are concentrated among focal organisations. Research on cyber physical supply chain networks similarly demonstrates that cascading resilience cannot be accurately represented through a single failure mode because different physical and cyber failures can interact within interconnected structures. Fu et al., (2026b) reinforce this concern by identifying network coupling and model realism as important unresolved challenges in contemporary cascading failure research. Digital integration therefore produces a strategic paradox similar to physical network connectivity. It enhances visibility, coordination, automation, and decision speed, but simultaneously creates new dependencies capable of transmitting disruption across organisational and technological boundaries. A digital failure can affect physical production, while physical disruption can reduce data availability and compromise digital decision systems. Cascading risk analysis must consequently treat technological infrastructure as an integral component of business interdependence rather than as an independent category of information technology risk. Corporate governance and ethical accountability provide an additional organisational foundation for assigning responsibility when interconnected risks cross functional and institutional boundaries (Liu & Renn, 2025).

Greater digital connectivity also changes the speed at which cascading consequences can emerge. Physical disruptions may require hours or days to propagate through inventory shortages and transportation delays, whereas failures affecting shared digital infrastructure can potentially influence multiple operations almost immediately. Zhou et al., (2026) demonstrate that information networks and resource supply networks interact in shaping overall resilience, showing that information dissemination itself influences how firms respond to emerging threats. Madzík et al., (2024), in their extensive review of supply chain risk and resilience research, identify system

security, critical infrastructure, information technology, complex network design, and operational mitigation as important interconnected research domains. The wider critical infrastructure literature reaches a comparable conclusion, recognising cascading failures as a consequence of dynamic interconnections both within and between infrastructure networks. These findings suggest that digital resilience cannot be confined to cybersecurity controls or system redundancy. Organisations must understand which physical activities depend on particular technologies, which partners share digital platforms, where data and decision dependencies are concentrated, and how technology failures could alter material or service flows. The domino effect of risk increasingly travels through both code and cargo. Effective governance must therefore map cyber physical dependencies together so that a disruption appearing initially technological is recognised for the operational, financial, reputational, and strategic consequences it may subsequently generate. The analytical focus must shift toward the connections through which pressure can move between firms, technologies, and infrastructure.

2.5 Resilience Recovery Capabilities Containing Cascading Business Failure Escalation

Resilience becomes strategically meaningful when an organisation can prevent disruption from acquiring sufficient momentum to destabilise the wider system. Traditional continuity planning often concentrates on restoring individual functions after failure, whereas cascading risk requires simultaneous attention to absorption, containment, adaptation, redistribution, and recovery across connected organisations. Roshani et al., (2024) classify resilient supply chain network mitigation strategies into proactive, reactive, and design quality capabilities, demonstrating that resilience depends on combinations of capacity, flexibility, network configuration, and response rather than a single intervention. Han and Um (2024) similarly identify inventory based strategies such as stockpiling, multisourcing, capacity reservation, and flexible supply contracts as mechanisms for strengthening supply chain resilience against disruption. Han and Um (2024) further connect risk mitigation strategies with resilience capability under global uncertainty and sustainability related supply chain risks. These contributions establish that redundancy should not be interpreted merely as inefficiency. Strategic buffers can provide the spare capacity required to prevent an initial disturbance from transferring excessive pressure to connected nodes. However, indiscriminate redundancy can be economically costly, making the placement and type of resilience capacity as important as its quantity. Effective containment therefore requires targeted protection of nodes and relationships whose failure would produce disproportionate systemic consequences. A systems view improves judgement by revealing when a locally sensible decision transfers delay, scarcity, or vulnerability to another node.

Recovery architecture is equally important because poorly designed restoration can redirect rather than eliminate cascading pressure. Hu et al., (2026) propose adaptive recovery strategies that recognise heterogeneous failure characteristics and changing operational states, moving beyond conventional approaches that treat recovery as a one time intervention. Cao et al., (2025) show that load redistribution rules influence how global container shipping networks respond to cascading failures, illustrating how recovery decisions at disrupted nodes can alter the resilience of the remaining network. Lin and Lin (2025) likewise approach resilience through multistate system reliability, recognising that supply chain performance cannot always be reduced to a simple operational or failed condition. Zhou et al., (2026) add that stronger risk awareness and structural adjustments can improve recovery capability and suppress risk propagation. The literature therefore points towards resilience as a dynamic system capability rather than a static reserve of resources.

Organisations must anticipate how recovery actions redistribute workloads, dependencies, information, and vulnerabilities throughout the network. The strongest response is not necessarily the fastest restoration of every disrupted node, but the configuration that preserves critical system functions while preventing secondary failures. Under this interpretation, resilience represents the capacity to absorb the first domino, restrict the movement of subsequent threats, adapt network relationships intelligently, and restore performance without creating the conditions for another cascade. Coordinated action at this stage is valuable because substitute capacity can disappear quickly once several firms react at the same time.

3. SYSTEMIC BUSINESS NETWORK VULNERABILITIES DRIVING CASCADING RISK ESCALATION

The most dangerous risks in modern business are increasingly those that refuse to remain where they originate. A disruption affecting one supplier, technology platform, transport corridor, financial institution, or infrastructure asset can alter operating conditions elsewhere and initiate secondary failures that are more damaging than the original event. Recent research confirms that cascading failures have become a critical source of instability within complex supply networks because interconnected nodes continuously exchange materials, information, capacity, and operational pressure (Tian et al., 2026). Ouyang et al., (2026) similarly demonstrate that systemic shocks within the global cobalt supply chain can propagate across countries and industries, illustrating how concentrated dependencies can convert local disturbances into broader supply consequences. The challenge becomes more serious when firms cannot observe the complete network in which they operate. Risk may therefore travel through suppliers, technologies, infrastructure, customers, or financial relationships that remain outside conventional organisational risk registers. Contemporary risk management must consequently confront five closely connected problems: hidden dependencies beyond direct business relationships, excessive concentration around critical nodes, behavioural responses that redirect disruption, cyber physical interdependence, and recovery strategies that unintentionally create new vulnerabilities. These challenges demonstrate why cascading risk cannot be governed effectively through isolated probability and impact assessments alone.

3.1 Hidden Dependency Structures Expanding Organisational Cascading Risk Exposure

What appears to be a diversified business system can remain dangerously concentrated beneath the surface. Organisations commonly understand direct suppliers, primary logistics providers, major customers, and internally controlled technologies, yet their exposure frequently extends several layers beyond these visible relationships. A supplier considered independent may depend on the same upstream manufacturer, raw material, digital platform, port, energy provider, or specialist technology as another supposedly alternative source. Namdar et al., (2024) demonstrate that cascading disruptions are shaped significantly by network structure, particularly because relationships among suppliers determine how disturbances spread after an initiating event. The broader literature on systemically important supply chains likewise shows that interdependencies between risk factors and network structures can create vulnerabilities that are difficult to detect through conventional firm level analysis (Qazi et al., 2025). Ouyang et al., (2026) provide a particularly relevant example through the global cobalt supply chain, where international production and trade dependencies allow regional shocks to generate cascading consequences across interconnected industries. These findings expose a major visibility problem. An organisation may believe that exposure has been diversified because contractual relationships are distributed across several suppliers, while critical dependencies remain concentrated further upstream. Conventional

risk registers can consequently underestimate the probability that several apparently independent business relationships will fail simultaneously when they share the same underlying dependency. For managers, visibility creates value only when decision rights, timely information, and escalation responsibilities are equally clear.

The strategic consequences of hidden dependency become particularly severe when alternative arrangements exist only on paper. Backup suppliers may lack independent upstream sources, alternative transport corridors may converge at the same infrastructure hub, and different cloud applications may depend on common digital infrastructure. Roshani et al., (2024) emphasise that resilient network design must consider disruption location together with structural mitigation strategies because resilience depends on how alternative pathways are actually configured rather than simply whether they exist. Namdar et al., (2024) similarly show that network modularity can restrict disruption spread between clusters while intensifying consequences within densely interconnected groups. This suggests that diversification should be assessed according to structural independence rather than numerical variety. Organisations therefore require deeper mapping of multi tier suppliers, shared technologies, logistics infrastructure, critical materials, data providers, financial dependencies, and specialised capabilities. Fessina et al., (2026) similarly demonstrate that systemic exposure can remain hidden when firm level network relationships are not visible. More recent work by Wang and Li (2026) on intelligent and resilient supply systems further reinforces the importance of capturing temporal and relational risk transmission rather than relying exclusively on static representations. Without such visibility, businesses may prepare multiple contingency options that ultimately fail together. The first contemporary issue is therefore not merely insufficient diversification, but insufficient understanding of whether diversification actually removes common points of failure.

3.2 Critical Node Concentration Transforming Efficiency Creating Systemic Fragility

Efficiency frequently encourages organisations to concentrate important activities within the most capable suppliers, hubs, systems, and partners. Such concentration can produce economies of scale, simplified coordination, stronger purchasing leverage, and greater operational consistency during stable conditions. The same architecture, however, can create disproportionate vulnerability when highly central nodes fail. Zeng et al., (2025) demonstrate that centralisation within cyber physical supply chain networks can improve coordination while simultaneously increasing structural fragility because critical information and operational functions become concentrated among focal organisations. Cao et al., (2025) reach a comparable conclusion within global container shipping networks, where disruption affecting structurally important ports can trigger load redistribution and cascading failure across interconnected routes. Shi et al., (2026) further show that supply chain resilience evolves through interactions among network topology, node capacity, operational load, and changing relationships rather than depending solely on individual firm robustness. The underlying problem is therefore one of asymmetric importance. Some nodes possess substantially greater systemic influence because large numbers of organisations depend on them directly or indirectly. Their failure can create simultaneous shortages, capacity pressures, information loss, transportation disruption, or financial stress across multiple network segments. Risk assessment frameworks that treat each node as equally significant can consequently misidentify where resilience investment is most urgently required. Under this logic, governance arrangements must change as dependencies, technologies, and resource constraints alter the pathways available to disruption.

Concentration also creates a difficult tradeoff because reducing dependency on critical nodes can increase costs and operational complexity. Firms may need additional suppliers, duplicated technologies, alternative logistics routes, spare capacity, decentralised inventories, or redundant information infrastructure to reduce exposure. Tsoulfas (2026) demonstrate within port resilience research that adaptive capacity, effective governance, stakeholder collaboration, and technological capability are increasingly important because infrastructure resilience is shaped by organisational and network interactions rather than physical assets alone. Tabatabaei et al., (2025) similarly emphasise the integration of risk within sustainable supply chain network design, reinforcing the need to evaluate network configuration through more than efficiency criteria. Roshani et al., (2024) extends this concern to regional resilience by highlighting the strategic role of supply chains within wider economic and security systems. These perspectives expose a structural dilemma. Concentration is not inherently undesirable, because strong hubs can provide significant productivity advantages. The danger arises when organisations become dependent on highly central nodes without understanding their systemic importance or establishing credible alternatives. Risk management should consequently distinguish between operationally efficient concentration and strategically excessive dependency. The domino effect becomes particularly destructive when the first falling node occupies a position capable of carrying many others with it. Decision makers need to identify which combinations of dependencies can transmit disruption across otherwise separate risk categories. This interpretation exposes the wider consequences of firm-level responses that appear efficient when evaluated in isolation.

3.3 Organisational Response Behaviour Intensifying Cascading Risk Propagation Dynamics

The actions taken after a disruption are not always stabilising. Firms attempt to protect themselves by securing alternative suppliers, increasing inventory, redirecting transportation, reserving capacity, changing production schedules, or competing for scarce resources. Individually rational actions can collectively create additional instability when many organisations respond simultaneously. Fu et al., (2026a) demonstrate that enterprise competition under incomplete information significantly affects cascading failure resilience because failed loads and scarce resources are redistributed according to competitive relationships rather than neutral network rules. Zhou et al., (2026) similarly show that risk propagation interacts with risk awareness and information transmission, meaning that organisational perceptions and responses can influence whether disruption accelerates or is contained. Liu and Renn (2025) places this phenomenon within the broader concept of polycrisis, arguing that contemporary risks increasingly interact across domains and amplify one another rather than developing as isolated events. These findings reveal that cascading risk is partly behavioural. Organisations do not simply experience disruption. They change the network through their reactions to it. When several firms simultaneously switch suppliers or transport routes, substitute capacity can become overloaded. When businesses increase precautionary inventories at the same time, temporary shortages can deepen. Responses intended to protect individual organisations can consequently redistribute pressure and create new points of instability elsewhere. Network-aware judgement helps managers anticipate where protective actions can unintentionally concentrate pressure on weaker partners. Collective visibility can reduce avoidable competition for scarce resources.

Incomplete or delayed information makes this problem more difficult because firms may respond aggressively before understanding whether disruption will persist or how other actors are reacting. Zhou et al., (2026) demonstrate that stronger information dissemination and risk awareness can

increase the threshold at which risk propagates, suggesting that communication quality can materially influence systemic resilience. Fu et al., (2026a) similarly find that incomplete information alters enterprise competition and cascading behaviour within dual layer supply networks. Liu and Renn (2025) further emphasise cross cutting supply chain risks and the difficulties created by weak communication across organisational boundaries. Wang and Li (2026) propose dynamic risk management approaches precisely because static decision systems struggle to account for temporal dependencies and rapidly evolving cascading paths. The implication is that information transparency has systemic value beyond ordinary coordination. Firms require mechanisms for sharing disruption severity, available capacity, expected recovery times, and changing operating conditions with strategically important partners. Without such mechanisms, each organisation may make reasonable decisions based on incomplete information while collectively accelerating network instability. Cascading threats therefore cannot be managed exclusively through independent organisational contingency plans. They require coordinated responses capable of recognising how one firm's recovery decision may alter the vulnerability of another. For digital dependencies, early coordination should connect technical incident signals with operational decisions before service degradation spreads. Shared protocols also clarify escalation when partner interests diverge.

3.4 Digital Integration Accelerating Hidden Cascading Risk Transmission Pathways

Digital connectivity has introduced a form of interdependence in which disruption can travel faster than traditional physical supply shortages. Cloud computing, enterprise platforms, industrial automation, shared databases, connected logistics systems, digital payment infrastructure, and artificial intelligence increasingly link organisations through common technological environments. Zeng et al., (2025) demonstrate that cyber physical supply chain systems can become more fragile as information and physical execution layers become increasingly coupled. Zeng et al., (2025) similarly develop a cascading failure model incorporating multiple cyber physical failure modes, demonstrating that recovery strategies need to account for interactions between technological and operational disruptions rather than treating them separately. Raptaki et al., (2025) extend this concern by examining automated cybersecurity impact propagation across business processes, illustrating how cyber incidents can transmit consequences through organisational dependencies. These developments change the temporal characteristics of cascading risk. A material shortage may take days to influence downstream production, whereas a shared platform outage, cyberattack, or corrupted information system can affect numerous organisations almost simultaneously. The initiating event may appear technological, yet its consequences can quickly become operational, financial, regulatory, and reputational. Cyber risk should therefore no longer be isolated within information technology departments when digital systems are embedded within the execution of critical business processes. Management practice must connect network visibility with explicit authority to intervene before pressure accumulates at critical nodes. Digital dependence also makes resilience an important dimension of technology adoption because operational growth can increase exposure to shared systems (Yusof, 2025b).

Digital concentration adds another dimension to this vulnerability. Organisations may diversify physical suppliers while simultaneously depending on the same cloud provider, cybersecurity platform, payment infrastructure, software ecosystem, or telecommunications network. Bae et al., (2026) specifically identifies systemic cyber risk as including cascading failures in which a single cyber incident propagates through interconnected supply chains and affects multiple organisations. Wang and Li (2026) likewise position digitalisation as a foundation for resilience while recognising

that highly interconnected digital ecosystems must support anticipation, absorption, adaptation, and recovery rather than simple automation. Wang et al., (2026) further propose intelligent approaches that integrate temporal risk information because cascading disruption evolves as node conditions change over time. Yet technological sophistication can create false confidence when firms interpret visibility tools as evidence that systemic exposure is controlled. Digital systems can improve detection while simultaneously increasing common dependency. Organisations should therefore map digital infrastructure alongside physical supply relationships, identify technologies supporting critical operations, assess concentration among shared providers, and examine how technology failure would propagate into production, logistics, customer service, finance, and partner operations. In interconnected business systems, one of the most dangerous dominoes may be invisible because it exists in software rather than in a warehouse or factory. Recovery decisions can then be tested against downstream capacity and dependency effects instead of being judged only by immediate restoration speed. Organisational resilience is consequently developed through repeated adjustment of network relationships, decision rights, and operational buffers.

3.5 Recovery Strategy Design Redistributing Residual Cascading Risk Exposure

Restoring operations quickly does not necessarily mean that systemic risk has been reduced. Recovery measures frequently redistribute loads, dependencies, inventories, transportation flows, and information requirements to alternative parts of the business network. If those alternative nodes possess limited capacity, the recovery process can simply move the cascade rather than stop it. Recent evidence address this problem through adaptive and risk recovery strategies that recognise heterogeneous failure characteristics and changing network conditions instead of assuming a single recovery mechanism. Shi et al., (2026) similarly demonstrate that resilience evolves over time as network topology, node capacity, relationships, and recovery potential change. Ren et al., (2026) show within land transport networks that cascading resilience is influenced by topology, coupling mechanisms, node criticality, and system adaptation. These findings expose a major weakness in conventional business continuity planning. Many plans focus on restoring the disrupted function without analysing the additional pressure imposed on the substitute function. An alternative supplier may technically exist but lack adequate capacity. A backup distribution centre may become congested once multiple facilities redirect inventory. Recovery therefore needs to be evaluated at system level rather than solely according to whether the originally disrupted activity has resumed. This interpretation positions resilience as a dynamic management capability rather than a fixed stock of contingency resources. Resilience assessment should reveal how individual exposures interact once capacity, information, or infrastructure becomes constrained.

Poorly sequenced recovery can also recreate the conditions for another failure. Ren et al., (2026) demonstrate through dynamic shipping network analysis that resilience against cascading effects changes continuously as traffic and network conditions evolve. Ouyang et al., (2026) similarly show that supply shocks can spread through international material networks when substitute flows create additional stress across already interconnected structures. Tsoulfas (2026) emphasise adaptive capacity and stakeholder collaboration as important components of resilience precisely because effective recovery requires coordination across interconnected actors. Y. Ren et al., (2026) extend this reasoning through the concept of cascading adaptation, demonstrating that transport resilience depends on adaptive responses across the wider network rather than isolated restoration. The most important contemporary issue is therefore not merely recovery speed but recovery architecture. Organisations need to evaluate where displaced demand, workloads, inventories, data flows, and

transportation requirements will move after disruption and whether receiving nodes possess sufficient capacity. Scenario planning should consequently include second and third order effects of recovery decisions. Effective resilience is achieved when restoration prevents further dominoes from falling rather than merely standing the first one back up.. Managers must distinguish ordinary dependencies from connections capable of carrying disruption into multiple business functions. The wider system must therefore be considered before local recovery actions are treated as evidence of resilience. Recovery choices must therefore consider consequences beyond immediate restoration.

4. STRATEGIC SYSTEM RECONFIGURATION STRENGTHENING CASCADING RISK RESILIENCE CAPABILITY

Business resilience acquires a fundamentally different meaning when disruption is capable of travelling across organisational boundaries. The preceding issues demonstrate that cascading threats cannot be interpreted simply as larger versions of conventional operational risks because their consequences are generated through interaction, dependency, behavioural response, and network transformation. Recent systematic evidence confirms that a relatively small number of node failures can initiate chain reactions capable of impairing an entire supply chain system, making cascading failure a distinct challenge for contemporary risk management. The strategic concern therefore extends beyond whether individual organisations possess sufficient protection against known threats. It concerns whether the wider system can absorb disruption without allowing pressure to migrate towards other vulnerable nodes. Gu et al., (2026) reinforce this perspective by conceptualising resilience through risk propagation and dynamic recovery rather than treating it solely as a static organisational characteristic. Similarly, Zelbi et al., (2026) demonstrate that systemic supply chain risk is closely connected to network topology and interfirm dependencies, indicating that resilience can potentially be improved by modifying the architecture through which firms are connected. These developments support a broader interpretation of cascading risk in which visibility, structural design, information transparency, digital interdependence, adaptive capacity, and recovery architecture collectively determine whether the first disruption remains manageable or develops into systemic instability.

4.1 Risk Visibility Evolution Building Strategic Dependency Intelligence Capability

Knowing direct suppliers is no longer equivalent to understanding organisational exposure. The current issues reveal that hidden dependencies can exist several layers beyond contractual relationships, allowing apparently diversified firms to remain vulnerable to common suppliers, infrastructure, technologies, transportation hubs, or resources. This distinction is strategically significant because conventional supplier mapping can create an illusion of diversification while leaving underlying concentration unchanged. Recent evidence identifies data acquisition and multi-source information integration as major priorities for improving the accuracy and timeliness of cascading failure analysis, particularly as supply networks become increasingly complex. Shi et al., (2026) similarly argue that supply chain viability requires dynamic network data and interaction models capable of representing interconnected relationships and changing responses to disruption. The implication is that risk visibility should evolve into what may be described as dependency intelligence, meaning the organisational capability to identify not only immediate partners but also the underlying assets, technologies, infrastructure, and relationships upon which those partners depend. Such intelligence changes risk assessment from a list of individual exposures into a map of shared vulnerabilities. Instead of asking whether several suppliers exist, managers should determine whether those suppliers genuinely provide independent pathways to critical resources. This

distinction is essential because numerical diversification offers little resilience when multiple alternatives ultimately converge upon the same vulnerable node. Such analysis clarifies whether an intervention genuinely contains risk or merely relocates it to a less visible part of the network.

Dependency intelligence also requires organisations to identify how exposure changes when business conditions evolve. Shi et al., (2026) demonstrate that supply chain resilience depends on the interaction of changing node capacities, load distributions, firm entry and exit, relationship turnover, and recovery potential, illustrating why static network representations can quickly become obsolete. Wang and Li (2026) likewise approach resilience from a supply network perspective, reinforcing the importance of understanding interconnected organisational relationships rather than concentrating exclusively on isolated firm capabilities. Das and Perona (2025) further show that the growing automation of supply chain risk management creates opportunities to integrate data, analytics, and decision processes more systematically across risk identification and response activities. Together, these studies suggest that visibility should become continuous rather than episodic. Organisations require living dependency maps that capture critical suppliers, common upstream sources, digital platforms, logistics corridors, financial relationships, specialised skills, infrastructure, and substitute capacity. Changes within these dependencies should trigger reassessment because a low importance node can become strategically critical when another connection fails. The managerial objective is therefore not complete visibility of every relationship, which may be impractical, but prioritised visibility of dependencies capable of transmitting disproportionate consequences. Such an approach would allow firms to identify the pathways through which the domino effect is most likely to travel before those pathways are activated by an actual disruption. This distinction supports more proportionate investment in systemic protection.

4.2 Efficiency Resilience Rebalancing Strengthening Structural Business Continuity Capacity

The pursuit of operational efficiency has produced business networks in which concentration is often economically attractive but strategically dangerous. Centralised sourcing, specialised production, consolidated logistics, common digital platforms, and dominant distribution hubs can lower costs and simplify coordination, yet they simultaneously concentrate systemic importance within a smaller number of nodes. Recent evidence demonstrates this tension in coupled centralised supply chain networks, where the concentration of critical decision and operational functions can improve coordination while increasing dependency on focal organisations. Recent evidence reaches a comparable conclusion in global container shipping, showing that cascading failure and load redistribution across highly interconnected ports significantly influence network resilience following disruption. Lin and Lin (2025) further conceptualise supply chains as multistate systems, indicating that resilience cannot be adequately understood through a simple distinction between functioning and failed networks. These findings challenge the assumption that the most efficient network configuration under normal operating conditions is necessarily the most desirable configuration under uncertainty. Structural resilience requires organisations to evaluate the consequences of concentration alongside its economic benefits. A supplier, port, technology platform, or distribution centre should therefore be assessed not only according to cost and performance but also according to the scale of disruption that its failure could transmit throughout the wider network. Operational intelligence is useful only when responsible managers can act quickly on credible information and predefined escalation triggers.

Resilience should nevertheless not become an argument for indiscriminate redundancy. Excessive duplication of suppliers, facilities, inventory, systems, and capacity can undermine competitiveness when additional resources provide little meaningful protection. The more sophisticated objective is selective redundancy, where buffers and alternatives are concentrated around dependencies capable of generating severe cascading consequences. Zelbi et al., (2026) demonstrate that systemic risk can be mitigated through supply network rewiring, suggesting that relatively targeted modifications to supplier and customer relationships may reduce systemic exposure without requiring wholesale network reconstruction. Recent evidence similarly find that recovery strategies should differentiate between core firms and interfirm capability disparities rather than applying uniform interventions throughout the network. Wang and Li (2026) provide further evidence that resilience can be strengthened through complementary organisational and supply chain mechanisms rather than through isolated measures. This supports a more economically disciplined resilience philosophy in which redundancy is treated as strategic capacity rather than unused capacity. Firms should identify nodes with high systemic importance and determine whether alternative sourcing, spare capacity, inventory buffers, modular processes, technological substitution, or network rewiring would meaningfully restrict disruption propagation. The appropriate balance between efficiency and resilience is therefore not achieved by maximising either objective. It is achieved by ensuring that efficiency gains do not depend on concentrations whose failure could impose consequences substantially greater than the savings they originally created.

4.3 Organisational Behaviour Coordination Preventing Systemic Response Amplification Effects

One of the most important insights emerging from cascading risk research is that organisations can unintentionally manufacture secondary disruption while attempting to protect themselves. When firms encounter shortages or capacity failures, they frequently increase orders, secure alternative suppliers, reserve transport capacity, accumulate inventory, redirect shipments, or compete for substitute resources. Each action may appear rational from the perspective of the individual organisation, yet simultaneous responses can create congestion, shortages, price escalation, capacity exhaustion, and additional network instability. Recent evidence demonstrates that competition and cooperation among enterprises influence load redistribution following failure and that incomplete information materially affects cascading resilience. Importantly, their findings indicate that greater information transparency can improve the ability of networks to resist cascading failures. Recent evidence reaches a related conclusion through their analysis of risk and risk awareness propagation, demonstrating that the interaction between information sharing and operational risk influences resilience across dual layer networks. These findings establish an important distinction between organisational resilience and systemic resilience. An action that strengthens one firm's immediate position may weaken the network if it transfers excessive pressure to organisations possessing lower capacity. Cascading risk therefore exposes the limitations of purely self-contained contingency planning. Governance must therefore evolve with the architecture of the business system instead of relying on static controls designed for earlier conditions. The practical priority is to understand where operational, digital, and supplier dependencies intersect and create common points of failure.

The practical implication is that coordination mechanisms should exist before disruption creates competition for scarce resources. Information sharing agreements, collaborative capacity arrangements, emergency sourcing protocols, joint escalation procedures, and predefined communication channels can reduce uncertainty when rapid decisions are required. Recent evidence

argues for an integrated framework combining forward looking risk warning with adaptive and reactive recovery strategies, supported by resource sharing, information exchange, and complementary capabilities among supply chain partners. Shi et al., (2026) similarly emphasise coordination between timely response and the danger of overreaction within interconnected supply networks. Huang et al., (2025) provide a broader systemic perspective from financial networks, demonstrating that risk co-contagion and network effects can cause systemic exposure to be misestimated when cascading mechanisms are inadequately considered. This principle is equally relevant to business networks because responses themselves become part of the risk transmission mechanism. Managers should therefore assess contingency decisions according to both direct organisational benefit and network consequences. Coordination does not require firms to surrender competitive autonomy. Rather, it requires recognition that during systemic disruption, information withholding and aggressive resource competition can destroy value for multiple actors, including the organisations attempting to protect themselves. Resilience becomes stronger when firms understand that controlling the second domino may require cooperation before the first one falls. Effective governance therefore maps the routes by which disruption can migrate rather than treating each registered risk as self-contained.

4.4 Digital Connectivity Governance Balancing Resilience Contagion Exposure Dynamics

Digitalisation has transformed the architecture of cascading risk by connecting information and physical operations more tightly than ever before. Integrated platforms, cloud infrastructure, automated production, blockchain applications, connected logistics, and digital decision systems can improve visibility and coordination, yet they can also create shared dependencies through which disruption propagates rapidly. Recent evidence demonstrates that deeper coupling between information decision systems and physical execution systems increases interdependence and can heighten fragility within centralised supply chain structures. This finding suggests that digital integration should not automatically be interpreted as resilience enhancement. A technology may strengthen operational control during normal conditions while simultaneously becoming a systemic point of dependency during failure. Das and Perona (2025) show that automation has considerable potential within supply chain risk management, particularly through the integration of technological tools across risk processes. Wang and Li (2026) similarly demonstrate that blockchain enabled supply chains can contribute to resilience and sustainability performance within logistics firms. The critical distinction lies in whether digitalisation expands adaptive options or concentrates essential processes around technologies whose failure cannot be readily substituted. Digital resilience should therefore be evaluated according to dependency architecture rather than technological sophistication alone. Managers can then distinguish actions that stabilise the system from those that protect one operation by increasing vulnerability elsewhere. Joint escalation arrangements are especially important where several partners depend on the same constrained supplier, route, or platform.

A stronger governance approach would treat every major digital implementation as both a capability and a potential transmission pathway. Firms should determine which operational activities depend on each critical system, which external organisations share the same technological infrastructure, how long operations can continue without it, and whether credible substitutes exist. Recent evidence identifies higher order network modelling and digital twin technologies as promising approaches for improving the simulation and prediction of cascading failures, indicating that digitalisation can itself provide tools for understanding systemic vulnerability. Gu et al., (2026) similarly develop resilience measurement around dynamic risk propagation, demonstrating the value of analysing how disruption

evolves rather than relying exclusively on static resilience indicators. Recent evidence further establish that information networks interact with resource supply networks in determining resilience, confirming that digital and operational structures should not be assessed independently. Organisations should consequently develop cyber physical dependency maps, technological concentration indicators, alternative communication arrangements, manual operating procedures for essential functions, data recovery capabilities, and scenario simulations involving simultaneous technological and operational failures. The objective is not to reduce digital connectivity, because doing so would sacrifice substantial productivity and visibility benefits. The objective is to ensure that digital connectivity increases the organisation's capacity to detect and contain cascading threats without becoming the mechanism through which those threats accelerate. Cross-organisational coordination should begin while response options remain available rather than after competing recovery actions have exhausted them.

4.5 Rapid Recovery Evolution Enabling Intelligent System Reconfiguration Capability

Recovery should be judged by the stability it restores, not merely by the speed at which disrupted operations resume. This distinction becomes essential in interconnected systems because restoring one node can transfer workloads and dependencies to other parts of the network that may already be operating near their limits. Recent evidence demonstrates that resilience is determined by the evolving interaction of node capacities, load distributions, network relationships, and recovery potential, highlighting the limitations of static recovery assumptions. Recent evidence similarly distinguish between adaptive and risk recovery strategies and demonstrate that resilience improves when proactive and reactive mechanisms operate together across changing node states. Recent evidence provides complementary evidence from container shipping, where the redistribution of loads following port disruption can materially alter the propagation of cascading failures throughout the network. These findings suggest that conventional metrics such as time to recovery may provide an incomplete picture of resilience. A firm may restore its own operations rapidly by shifting production, orders, shipments, or data processing elsewhere while simultaneously increasing the probability that another node will fail. Recovery effectiveness should therefore include the capacity of the wider network to absorb the consequences of restoration decisions without initiating another cascade. Effective governance therefore couples visibility with decision authority, response ownership, and information that arrives early enough to matter. Such governance links technical resilience directly with operational continuity priorities.

This perspective supports a transition from recovery planning towards intelligent system reconfiguration. Instead of asking only how quickly the original operating model can be restored, managers should determine which configuration can preserve critical functions most safely under changed conditions. Gu et al., (2026) explicitly incorporate dynamic recovery into resilience measurement and emphasise the cascading effects of risk propagation across alternative scenarios. Cao et al., (2025) demonstrates the practical significance of this problem within global container shipping, where disruptions affecting Middle Eastern maritime choke points can produce systemic cascading consequences as vessels are rerouted through alternative pathways. Zelbi et al., (2026) further demonstrate that network rewiring can reduce systemic supply chain risk, providing evidence that changing relationships may sometimes produce greater resilience than restoring the original configuration unchanged. Recovery strategies should consequently evaluate substitute capacity, receiving node vulnerability, resource redistribution, temporary network concentration, and the possibility that emergency arrangements themselves become new critical dependencies. Scenario

analysis should extend beyond the first recovery decision to examine its second and third order consequences. The most resilient organisation is therefore not necessarily the one that returns fastest to its previous state. It is the one capable of reconfiguring relationships, resources, technologies, and operating priorities without transferring destabilising pressure elsewhere in the system. Scenario-based governance gives managers a clearer basis for deciding when to isolate, reroute, substitute, or deliberately slow a recovery action.

5. GOVERNANCE PATHWAYS STRENGTHENING CASCADING BUSINESS RISK CONTAINMENT CAPABILITY

Preventing the first disruption is no longer a sufficient ambition for risk management. The more consequential managerial challenge is ensuring that an initial failure does not acquire the connectivity, capacity, and momentum required to destabilise the wider business system. The discussion demonstrates that cascading threats emerge through several interacting mechanisms, including hidden dependencies, structural concentration, competitive responses, digital interdependence, and poorly configured recovery decisions. Recent evidence establish that network architecture significantly influences both the spread and severity of cascading disruption, while Recent evidence demonstrates that resilient supply chain design requires combinations of proactive, reactive, and structural mitigation capabilities. More recent evidence strengthens this argument. Recent evidence shows that recovery effectiveness depends on heterogeneous organisational conditions and adaptive responses, while Recent evidence demonstrates that systemic supply chain risk can be reduced by deliberately modifying network relationships. These findings suggest that organisations need to move beyond conventional risk registers towards an architecture of systemic resilience capable of detecting propagation pathways, reducing critical concentrations, coordinating responses, governing digital dependencies, and reconfiguring operations intelligently during disruption. Five strategic priorities are therefore proposed to convert cascading risk management from reactive containment into a deliberate capability for protecting interconnected business systems.

5.1 Dynamic Dependency Intelligence Strengthening Business Ecosystem Risk Visibility

Organisations should first replace conventional supplier visibility with dynamic dependency intelligence capable of revealing where seemingly independent business relationships ultimately converge. Risk assessments commonly identify direct suppliers, logistics providers, technologies, and customers while overlooking common upstream resources and infrastructure that can create simultaneous failures. Recent evidence demonstrates that cascading disruption is strongly influenced by supply network architecture and identify nexus suppliers whose disruption can exert disproportionate operational consequences. Their empirical analysis of 2,598 firms and suppliers across 51 countries illustrates why structural position matters considerably more than simple supplier counts when evaluating vulnerability. Fessina et al., (2026) similarly emphasise that quantifying system wide consequences from local disruption requires detailed knowledge of network topology because systemic risk is highly sensitive to the underlying configuration of production relationships. Organisations should consequently construct dependency maps extending beyond Tier 1 relationships to identify shared manufacturers, critical raw materials, transportation corridors, ports, digital platforms, utilities, financial providers, specialist knowledge, and infrastructure. These maps should distinguish nominal alternatives from genuinely independent alternatives. Two suppliers located in different countries may appear diversified while depending on the same semiconductor manufacturer, shipping route, technology provider, or specialised material. Such hidden

convergence represents a form of systemic concentration that conventional supplier databases can easily overlook. Dependency intelligence would enable organisations to identify where one failure could activate multiple apparently unrelated exposures simultaneously.

The value of dependency mapping, however, depends on whether it remains current as relationships and operating conditions change. Static maps become progressively less useful when firms change suppliers, capacities fluctuate, transport routes shift, technologies are replaced, and new interdependencies emerge. Organisations should therefore establish recurring network reviews supported by procurement, operations, logistics, information technology, finance, and enterprise risk functions. Critical dependencies can be assigned indicators reflecting concentration, substitutability, recovery time, capacity availability, and propagation potential. Automated monitoring should then identify material changes requiring managerial review. Recent evidence demonstrates that resilient network design requires mitigation strategies to be aligned with the location and characteristics of disruption rather than applied uniformly across the network. Fessina et al., (2026) further show why realistic firm level network information is important for estimating systemic consequences that cannot be captured adequately through aggregate sector relationships. The managerial objective should therefore be prioritised visibility rather than impossible attempts to map every connection equally. Organisations need the deepest visibility around dependencies whose failure would generate substantial second and third order consequences. Risk governance would consequently progress from asking which suppliers are critical to asking which combinations of relationships, resources, infrastructure, and technologies could allow a single disturbance to become a systemic event. Systemic resilience depends on seeing the network of dependencies that links apparently separate operational vulnerabilities. Regular mapping also reveals dependencies created by recent network changes.

5.2 Critical Connection Redesign Preventing Cascading Risk Propagation Escalation

Network architecture should be treated as a controllable component of risk exposure rather than an inherited operational condition. Organisations frequently accept existing supplier, customer, logistics, and technology relationships because they perform efficiently under normal conditions, yet these configurations may contain structural weaknesses that become visible only during disruption. Recent evidence provides particularly important evidence by demonstrating that systemic supply chain risk can be significantly reduced through network rewiring. Their findings show that carefully modifying supplier and customer relationships can alter the pathways through which failures propagate without requiring the complete reconstruction of the supply system. Recent evidence similarly demonstrate that modularity has contrasting effects on cascading disruption. Greater separation between modules can restrict the overall spread of disruption, while excessive connectivity within modules can intensify its local severity. These findings suggest that organisations should evaluate network design according to both operational performance and propagation potential. Critical relationships should be assessed for dependency concentration, network centrality, alternative pathways, spare capacity, and the consequences of simultaneous failure. Where excessive concentration exists, organisations can consider additional suppliers, regional diversification, modular operating structures, alternative transportation corridors, decentralised inventory, or substitute technologies. The purpose is not to eliminate connectivity, because connectivity remains essential for efficiency and coordination. The objective is to prevent strategically important connections from becoming uncontrollable transmission channels. Viewing

decisions through their network effects makes hidden transfers of risk more visible before they become secondary disruptions.

Structural resilience should also be economically selective. Attempting to duplicate every supplier, facility, system, and logistics route would impose substantial cost while providing limited additional protection against many disruptions. Roshani et al., (2024), through their systematic review, classify resilient network strategies across proactive, reactive, and supply chain design quality capabilities and identify additional capacity and flexibility as important mechanisms for mitigating disruption. A robust network design study published in 2024 similarly demonstrates the importance of incorporating uncertain disruption risk directly into supply chain network configuration rather than treating resilience as an adjustment made after the network has already been optimised for efficiency. Recent evidence further demonstrate that topology and load redistribution jointly influence resilience within the global container shipping network, confirming that structural position and operational capacity must be evaluated together. Organisations should consequently allocate redundancy according to systemic importance. Nodes with high propagation potential may justify dual sourcing, reserved capacity, emergency inventory, alternative digital infrastructure, or prequalified substitutes, whereas peripheral nodes may require less costly arrangements. This creates precision resilience, where investment is concentrated at locations capable of preventing the greatest amount of cascading damage. Such an approach preserves competitiveness because resilience expenditure is directed towards structural vulnerabilities rather than distributed indiscriminately throughout the organisation. Embedding these discussions in routine governance allows managers to intervene before a local disruption acquires systemic momentum.

5.3 Coordinated Response Protocols Preventing Disruption Driven Resource Competition

Cascading risk management should recognise that organisational behaviour after disruption can become part of the disruption itself. When several firms simultaneously compete for substitute suppliers, transportation capacity, inventory, labour, or critical materials, individual attempts at protection can intensify shortages and transfer instability across the network. Recent evidence demonstrates that enterprise competition and incomplete information significantly affect cascading failure resilience because resources following organisational failure are redistributed according to competitive and cooperative relationships rather than simple proximity. Their findings have substantial managerial implications because contingency plans developed independently by different organisations may rely on the same supposedly available emergency resources. A backup supplier capable of supporting one customer may become incapable of supporting ten customers that activate contingency contracts simultaneously. Organisations should therefore identify strategic partners with whom coordinated disruption protocols are necessary before an emergency occurs. Such protocols can define information sharing responsibilities, emergency capacity arrangements, escalation procedures, allocation principles, alternative sourcing mechanisms, and expected communication frequency. Coordination should be particularly strong around scarce resources whose sudden demand is likely to increase across multiple organisations during a common disruption. This does not require businesses to disclose commercially sensitive information indiscriminately. Instead, it requires predefined rules governing the minimum information necessary to prevent uncertainty and competitive behaviour from transforming a manageable shortage into a wider systemic crisis. Managers need more than dashboards; they require agreed authority, reliable signals, and clear accountability for cross-boundary intervention.

Joint scenario exercises should complement formal response protocols because organisations need to understand how their individual contingency decisions interact. Simulations can examine what occurs when several firms activate alternative suppliers simultaneously, reroute shipments through the same port, increase safety stocks, reserve limited transportation capacity, or migrate operations to shared digital infrastructure. Recent evidence demonstrates the importance of load redistribution rules in determining resilience following cascading failures, illustrating that the destination of displaced operational pressure can materially change system outcomes. Recent evidence likewise emphasise adaptive recovery across different organisational states rather than uniform recovery interventions. Recent evidence further show that incomplete information influences competition and cascading behaviour, reinforcing the value of transparency during disruption. Organisations should consequently establish cross functional crisis teams capable of evaluating not only immediate operational restoration but also the network consequences of proposed actions. Procurement should consider whether substitute sourcing will exhaust shared capacity, logistics teams should evaluate congestion created by rerouting, and finance should assess whether emergency purchasing transfers stress into cash flow or supplier solvency. The governing principle should be that a contingency action is incomplete until its downstream consequences have been evaluated. Coordinated response therefore becomes a mechanism for preventing rational individual decisions from producing irrational collective outcomes. This approach makes resilience investment more selective by linking intervention choices to propagation pathways and changing network conditions.

5.4 Digital Interdependence Governance Strengthening Strategic Continuity Risk Control

Digital resilience should be elevated from a technical concern to an enterprise level component of cascading risk governance. Modern organisations depend on interconnected cloud services, enterprise systems, automation platforms, digital payment infrastructure, data exchanges, communications networks, and software providers that frequently support multiple business functions simultaneously. This concentration creates operational leverage during stable conditions but can generate extensive consequences when shared technologies fail. Organisations should therefore develop cyber physical dependency maps connecting critical digital assets directly to the business processes, suppliers, customers, and physical operations they support. The purpose is to reveal consequences that conventional cybersecurity assessments may overlook. A platform outage should not be evaluated only according to system downtime, for example, but also according to its potential effects on order processing, production scheduling, warehouse execution, transportation, supplier communication, financial transactions, and customer fulfilment. Fessina et al., (2026) demonstrate more broadly that systemic risk depends sensitively on network structure, a principle equally relevant to interconnected digital dependencies. Roshani et al., (2024) reinforce the need for flexibility and structural mitigation within resilient networks rather than dependence on isolated response measures. Digital continuity planning should therefore identify shared providers, common technological dependencies, single points of authentication, concentrated data infrastructure, and processes incapable of functioning manually when systems become unavailable. Continuous renewal of resilience capability is necessary because the network that absorbs one disruption may not be the network that confronts the next.

Technology should simultaneously be used to improve the organisation's ability to anticipate cascading behaviour. Digital twins, network analytics, real time monitoring, artificial intelligence, and simulation technologies can enable managers to explore how failures might propagate before real disruptions occur. Such tools are particularly valuable when dependencies are too numerous and

dynamic for conventional risk workshops to evaluate effectively. The objective should not be technological sophistication for its own sake but improved decision quality regarding propagation pathways and intervention points. Organisations can develop simulations in which critical suppliers fail, digital platforms become unavailable, transportation nodes close, or several disturbances occur simultaneously. Resulting scenarios should identify which nodes become overloaded, which alternative pathways remain viable, and where secondary failures are likely to emerge. Gu et al., (2026) demonstrate the analytical value of combining network topology with operational flow when evaluating cascading resilience, rather than relying on structural connectivity alone. Hu et al., (2026) similarly incorporate multiple failure modes and adaptive operational states when analysing resilience, demonstrating why realistic models need to represent heterogeneity rather than assume identical responses across all nodes. Digitalisation can therefore become both a source of systemic exposure and an instrument for controlling it. Effective governance requires organisations to reduce dangerous technological concentration while simultaneously exploiting digital intelligence to detect weak signals, simulate chain reactions, and intervene before cascading pressure reaches critical thresholds.

5.5 Systemic Recovery Quality Strengthening Long Term Resilience Performance

Recovery performance should no longer be evaluated primarily according to how quickly an organisation returns to its previous operating state. Such a measure can reward decisions that restore one function rapidly while transferring instability elsewhere. Hu et al., (2026) demonstrate that cascading resilience depends on adaptive and risk recovery strategies across heterogeneous organisational states, indicating that effective recovery is a continuous and differentiated process rather than a single restoration action. Cao et al., (2025) similarly demonstrate that load redistribution following failure affects subsequent resilience because displaced pressure can generate additional failures if receiving nodes lack sufficient capacity. Organisations should therefore introduce the concept of systemic recovery quality, which evaluates whether restoration preserves critical business functions without creating disproportionate secondary vulnerability. Recovery assessments should examine the capacity utilisation of alternative suppliers, congestion at substitute logistics hubs, inventory depletion, technological concentration, employee workload, financial consequences, and the sustainability of temporary arrangements. A business that restores production within twenty four hours by transferring all demand to one alternative supplier may appear resilient according to conventional recovery metrics, yet it may have created a more dangerous concentration than existed before the disruption. Recovery decisions should consequently be evaluated through both immediate performance restoration and the risk profile of the resulting network configuration. This changes resilience from a race back to normality into a disciplined process of restoring stability without preparing the conditions for the next failure.

Organisations should also accept that returning to the original network configuration may not always represent the strongest recovery outcome. Severe disruption can reveal dependencies that were economically efficient but strategically fragile, creating an opportunity to redesign relationships rather than reconstruct the same vulnerabilities. Zelbi et al., (2026) demonstrate that network rewiring can materially reduce systemic risk, providing strong evidence that changes to supplier and customer relationships can improve resilience. Roshani et al., (2024) likewise show that resilient supply chain network design integrates proactive, reactive, and design capabilities, supporting the view that recovery and structural improvement should operate together. Namdar et al., (2024) further demonstrate that network modularity and the identification of nexus suppliers can help organisations

understand where structural interventions may limit future cascading consequences. Post disruption reviews should therefore examine which dependencies failed, which alternatives became overloaded, which information arrived too late, which emergency resources were shared with competitors, and which temporary solutions proved unexpectedly effective. Lessons should then influence sourcing policies, network configuration, technology architecture, inventory positioning, contractual arrangements, and future scenario planning. Recovery becomes strategically valuable when the system emerging after disruption is less susceptible to the same cascading pathway than the system that existed before it. Resilience is consequently not restoration alone. It is the capacity to learn from disruption and convert recovery into structural improvement. Post-disruption learning should reshape future network design and contingency choices.

A final recommendation is to institutionalise cascading risk governance within strategic decision making rather than activating it only during crises. Organisations should establish a recurring systemic resilience review that brings together enterprise risk management, procurement, operations, supply chain, logistics, information technology, finance, strategy, and business continuity functions. The review should examine changes in critical dependencies, concentration levels, nexus nodes, substitute capacity, digital exposure, recovery arrangements, and network propagation scenarios. Namdar et al., (2024) demonstrate that identifying structurally important nexus suppliers can support proactive mitigation, while Fessina et al., (2026) show that realistic systemic risk estimation depends heavily on understanding underlying firm level network patterns. Zelbi et al., (2026) further demonstrate that network structure itself can become an intervention variable through strategic rewiring. Roshani et al., (2024) reinforce the importance of combining multiple mitigation capabilities rather than depending on a single resilience strategy. These findings collectively support a fundamental shift in managerial thinking. Risk governance should no longer ask only whether individual threats have been identified and controlled. It should ask whether the business system has been designed so that inevitable failures remain containable. Through dynamic dependency intelligence, precision resilience, coordinated response protocols, digital interdependence governance, and systemic recovery quality, organisations can progressively reduce the probability that one disruption will activate another. The ultimate objective is not to create a business system in which no domino ever falls. It is to create one in which the fall of a single domino encounters sufficient visibility, structural separation, adaptive capacity, and coordinated intervention to prevent the entire system from following it.

6. CONCLUSION

A single disruption becomes truly dangerous when the system around it allows consequences to multiply. The analysis developed in this study demonstrates that cascading risk is not defined merely by the severity of an initiating event, but by the architecture of interdependence through which operational pressure, information failure, capacity shortages, technological disruption, and behavioural responses are transmitted. Modern organisations operate within networks where suppliers, logistics infrastructure, digital platforms, financial relationships, and strategic partners are increasingly connected, making it possible for apparently local disturbances to evolve into systemic instability. Hidden dependencies further complicate this exposure because contractual diversification may conceal common upstream suppliers, shared technologies, transportation corridors, or infrastructure capable of failing simultaneously. The strategic significance of risk therefore extends beyond identifying individual threats and estimating their probability and impact. Organisations must understand how vulnerabilities are connected, where systemic importance is

concentrated, and which relationships possess the capacity to transmit disruption across organisational boundaries. This perspective fundamentally repositions risk management from the protection of isolated organisational components towards the governance of interconnected systems in which resilience depends on containing propagation as much as preventing initial failure.

The study further establishes that interconnectedness carries a strategic paradox. The same network structures that generate efficiency, coordination, specialisation, digital integration, and global reach can also create pathways through which disruption accelerates. Concentrated suppliers and infrastructure can deliver considerable operational advantages, yet their failure may expose multiple organisations simultaneously. Digital technologies enhance visibility and decision speed while also generating cyber physical dependencies capable of transmitting disruption almost instantaneously. Organisational responses introduce another layer of complexity because actions intended to protect an individual firm can redistribute pressure across the wider network and generate additional instability. Consequently, resilience cannot be achieved through redundancy, technology, information sharing, or contingency planning in isolation. It requires an integrated architecture combining dynamic dependency intelligence, selective structural protection, coordinated response protocols, digital interdependence governance, and adaptive recovery. The recommendations developed in this study accordingly emphasise identifying systemic dependencies, redesigning critical connections, improving coordination before resources become contested, and evaluating technological infrastructure according to both its operational contribution and its potential role as a transmission mechanism. Such measures transform resilience from a defensive reserve into an active capability for governing how disruption moves through the system.

The decisive measure of resilience should ultimately be whether the organisation can stop one failure from determining the fate of everything connected to it. Rapid recovery remains important, but returning quickly to operations provides little strategic advantage when restoration merely transfers vulnerability to alternative suppliers, technologies, facilities, or logistics nodes. The article therefore advances a broader conception of systemic recovery quality in which successful restoration must preserve essential functions while avoiding the creation of new concentrations and secondary failures. The analysis also demonstrates that disruption can provide an opportunity for intelligent reconfiguration, particularly when network relationships that previously appeared efficient are revealed to be structurally fragile. Effective risk governance should consequently become continuous, cross functional, and network oriented, incorporating procurement, operations, logistics, information technology, finance, strategy, and business continuity into recurring assessments of dependencies, propagation pathways, substitute capacity, and recovery arrangements. The enduring lesson of the domino effect is therefore not that every disruption can be prevented. It is that the consequences of disruption can be shaped by how intelligently business systems are designed, connected, monitored, and reconfigured. Resilient organisations will be distinguished not by their ability to ensure that no domino ever falls, but by their capacity to ensure that when one does, the chain reaction ends there.

DECLARATIONS**1. Acknowledgement**

The authors gratefully acknowledge the academic support and resources provided by the Institute of Graduate Studies, Universiti Poly-Tech Malaysia (UPTM). Appreciation is also extended to scholars whose published works provided valuable foundations for the conceptual examination of cascading risk, systemic vulnerability, business network interdependence, risk propagation, 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

Ahmad Fauzi Ahmad Zaini: Conceptualization, literature review, development of the conceptual framework and arguments, manuscript preparation, and critical revision.

Airuddin Ahmad: Literature synthesis, conceptual development, scholarly interpretation, critical review, and manuscript refinement.

Both 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

- Abdullah, F. I., Yusof, M. S., & Abu Seman, S. (2020). Strategic warehouse management and supply chain performance in a changing business environment. *The Asian Journal of Professional & Business Studies*, 1(2), 73–89. <https://doi.org/10.61688/ajpbs.v1i2.155>
- Bae, K., Jung, K., & Zhang, L. (2026). Systemic cyber risks and insurance regulatory capital. The Geneva Papers on Risk and Insurance Issues and Practice. <https://doi.org/10.1057/s41288-026-00394-3>
- Binh, A. D. T., Asif, M. S., Fan, Y., Cam, H. L. T., & Quang, H. T. (2025). The domino effect of risks on supply chain performance in disruptive times. *International Journal of Construction Management*. <https://doi.org/10.1080/15623599.2025.2530641>
- Cao, Y., Xin, X., Jarumaneeroj, P., Li, H., Feng, Y., Wang, J., Wang, X., Pyne, R., & Yang, Z. (2025). Data driven resilience analysis of the global container shipping network against two cascading failures. *Transportation Research Part E: Logistics and Transportation Review*, 193, 103857. <https://doi.org/10.1016/j.tre.2024.103857>
- Das, S. K., & Perona, M. (2025). Supply chain risk management automation: A literature review. *Electronic Markets*, 35, 104. <https://doi.org/10.1007/s12525-025-00844-1>
- Echefaj, K., Charkaoui, A., Cherrafi, A., Garza-Reyes, J. A., & Ivanov, D. (2024). Design of resilient and viable sourcing strategies in intertwined circular supply networks. *Annals of Operations Research*, 337, 459–498. <https://doi.org/10.1007/s10479-024-05873-1>

- Fessina, M., Cimini, G., Squartini, T., Astudillo-Estévez, P., Thurner, S., & Garlaschelli, D. (2026). Inferring firm level supply chain networks with realistic systemic risk from industry sector level data. *Scientific Reports*, 16, 19848. <https://doi.org/10.1038/s41598-026-47883-y>
- Fu, X., Tian, M., Liu, X., Wu, S., & Peng, R. (2026a). Cascading failure resilience of dual layer supply chain networks under enterprise competition with incomplete information. *Reliability Engineering & System Safety*, 266, 111735. <https://doi.org/10.1016/j.ress.2025.111735>
- Fu, X., Tian, M., Liu, X., Wu, S., & Peng, R. (2026b). Systematic review and future perspectives on cascading failures in supply chains: Modeling and optimization. *Reliability Engineering & System Safety*, 270, 112150. <https://doi.org/10.1016/j.ress.2025.112150>
- Gu, X., Yang, Y., Li, J., Wang, X., Li, J., Wu, D., & Xu, X. L. (2026). A novel resilience measurement model for supply chains based on risk propagation. *International Journal of Production Economics*, 297, 110013. <https://doi.org/10.1016/j.ijpe.2026.110013>
- Han, N., & Um, J. (2024). Risk management strategy for supply chain sustainability and resilience capability. *Risk Management*, 26, Article 6. <https://doi.org/10.1057/s41283-023-00138-w>
- Hu, X., Li, X., Wang, C., Yao, C., & Lim, M. K. (2026). Adaptive and risk recovery strategies for enhancing supply chain network resilience: A cascading failure perspective. *Annals of Operations Research*. <https://doi.org/10.1007/s10479-026-07070-8>
- Huang, C., Miao, H., Yang, X., Cao, J., & Yang, H. (2025). Cascading failure, financial network and systemic risk. *The North American Journal of Economics and Finance*, 80, 102505. <https://doi.org/10.1016/j.najef.2025.102505>
- Ivanov, D. (2023). Collaborative emergency adaptation for ripple effect mitigation in intertwined supply networks. *Annals of Operations Research*. <https://doi.org/10.1007/s10479-023-05408-0>
- Lin, K. Y., & Lin, Y. K. (2025). An algorithm for assessing a multistate resilience supply chain network in terms of system reliability. *Annals of Operations Research*. <https://doi.org/10.1007/s10479-025-06769-4>
- Liu, H., & Renn, O. (2025). Polycrisis and systemic risk: Assessment, governance, and communication. *International Journal of Disaster Risk Science*. <https://doi.org/10.1007/s13753-025-00636-3>
- Madzik, P., Falát, L., Copuš, L., Valeri, M., & Čarnogurský, K. (2024). Resilience in supply chain risk management in disruptive world: Rerouting research directions during and after pandemic. *Annals of Operations Research*. <https://doi.org/10.1007/s10479-024-06126-x>
- Namdar, J., Blackhurst, J., Zhao, K., & Song, S. (2024). Cascading disruptions: Impact of modularity and nexus supplier predictions. *Journal of Supply Chain Management*, 60(3), 18–38. <https://doi.org/10.1111/jscm.12326>
- Ouyang, X., Liu, L., Liu, Q., Chen, W., Wang, C., Pang, X., He, C., & Liu, G. (2026). Systemic risks and cascading dynamics in the global cobalt supply chain. *Environmental Science and Ecotechnology*, 29, 100654. <https://doi.org/10.1016/j.ese.2025.100654>
- Qazi, A. (2025). Systemically important supply chains in crisis: Mapping disruptions and global ripple effects. *Natural Hazards Research*. <https://doi.org/10.1016/j.nhres.2025.09.003>

- Raptaki, M., Stergiopoulos, G., & Gritzalis, D. (2025). Automated cybersecurity impact propagation across business processes using process mining techniques. *International Journal of Information Security*, 24, Article 129. <https://doi.org/10.1007/s10207-025-01040-0>
- Ren, W., Ma, F., Shang, Z., Wang, L., Liu, W., Liu, Q., Li, J., & Ko, J. (2026). Land transport network resilience to cascading failures: A systematic literature review of modeling, evaluation, and recovery. *Journal of Traffic and Transportation Engineering English Edition*, 13(2), 491–523. <https://doi.org/10.1016/j.jtte.2026.03.001>
- Roshani, A., Walker-Davies, P., & Parry, G. (2024). Designing resilient supply chain networks: A systematic literature review of mitigation strategies. *Annals of Operations Research*, 341, 1267–1332. <https://doi.org/10.1007/s10479-024-06228-6>
- Santos, C. R. D., Oliveira, U. R. D., & Aprigliano, V. (2025). Supplier risk in supply chain risk management: An updated conceptual framework. *Applied Sciences*, 15(13), 7128. <https://doi.org/10.3390/app15137128>
- Shi, J., Tang, Z., Zhan, X. X., & Liu, C. (2026). Temporal modeling and resilience analysis of supply chain networks under cascading failures. *Reliability Engineering & System Safety*, 266, 111763. <https://doi.org/10.1016/j.ress.2025.111763>
- Stentoft, J., & Mikkelsen, O. S. (2024). Towards supply chain resilience: A structured process approach. *Operations Management Research*, 17(4), 1421–1443. <https://doi.org/10.1007/s12063-024-00513-0>
- Tsoulfas, G. T. (2026). Port resilience: A systematic literature review. *Maritime Economics & Logistics*, 28, 388–408. <https://doi.org/10.1057/s41278-025-00326-3>
- Wang, Z., & Li, Y. (2026). Artificial intelligence for intelligent, resilient, and sustainable supply chain management. *International Journal of Computational Intelligence Systems*, 19, Article 237. <https://doi.org/10.1007/s44196-026-01349-1>
- 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>
- Yusof, M. S., & Razali, H. (2020). Navigating organisational uncertainty through risk perception and managerial judgement. *The Asian Journal of Professional & Business Studies*, 1(1), 76–92. <https://doi.org/10.61688/ajpbs.v1i1.69>
- Yusof, M. S., Rahman, S. N. M. S. A., Seman, S. A., & Zahari, F. M. (2025). The impact of warehouse management systems on supply chain resilience and business competitiveness in a rapidly changing global market. *International Journal of Business and Technology Management*, 7(2), 332–345.
- Zelbi, G., Ialongo, L. N., & Thurner, S. (2026). Systemic risk mitigation in supply chains through network rewiring. *Scientific Reports*, 16, 12334. <https://doi.org/10.1038/s41598-026-42549-1>

- Zeng, Z., Wang, N., Xu, D., & Chen, R. (2025). Cascading failure modeling and resilience analysis of coupled centralized supply chain networks under hybrid loads. *Systems*, 13(9), 729. <https://doi.org/10.3390/systems13090729>
- Zhou, J., Lv, W., Wang, J., Zheng, R., & Yang, X. (2026). Impact of risk and risk awareness coupling propagation on the resilience of supply chain in a dual layer network. *Reliability Engineering & System Safety*, 265, 111475. <https://doi.org/10.1016/j.res.2025.111475>