Transportation Research Part E 151 (2021) 102347

Contents lists available at ScienceDirect

Transportation Research Part E

journal homepage: www.elsevier.com/locate/tre

Supply- and cyber-related disruptions in cloud supply chain firms: Determining the best recovery speeds

Li-Ming Chen [a,*], Wei-Lun Chang [b]

[a] Department of Business Administration, National Chengchi University, No. 64, Sec. 2, ZhiNan Road, Wenshan District, Taipei 11605, Taiwan, ROC
[b] Department of Business Management, National Taipei University of Technology, 1, Sec. 3, Zhongxiao E. Road, Taipei, Taiwan, ROC

ARTICLE INFO

Keywords:
Supply chain
Cloud computing
Disruption
Recovery
Cellular automata simulation

ABSTRACT

This study investigated the speeds (i.e., radical, incremental, relaxed benchmarking, rigorous benchmarking, matching, and market-driven) of firms' recovery from supply- and cyber-related disruptions in cloud supply chains (SCs). Supply-related disruptions downgrade the firm's operational capabilities (e.g., production capacity and labor supply), and cyber-related disruptions reduce its intangible capabilities (e.g., reputation, brand image, and public trust). This study introduced a cellular automata (CA) simulation model to determine the best recovery speeds following the loss of operational and intangible capabilities. Furthermore, to investigate the impact of cloud adoption on an SC firm's best speeds of recovery from supply-related disruptions, we compared firms that had adopted the cloud with those using the on-site data centers.

1. Introduction

In 2020, the COVID-19 pandemic severely disrupted the global supply chain (SC). Factories located at the epicenter of the outbreak in Wuhan, China, were forced to close to prevent the virus from spreading, and factories outside of the epicenter in China and worldwide were also affected. For example, some factories outside the epicenter experienced labor shortages due to worker furloughs, and others faced shortages of parts and raw materials; thus, they had to halt production (Haren and Simch-Levi, 2020).

Disruptions to the normal supply of goods and materials are a common problem in SC firms (Sheffi and Rice, 2005; Craighead et al., 2007; Kim et al., 2015). Such supply-related disruptions have often occurred during 2010–2020, including during the 2011 Tōhoku earthquake and tsunami in Fukushima, Japan; the devastating 2011 floods in Thailand; and the 2020 COVID-19 pandemic. Supply-related disruptions reduce operational capabilities through physical damage to manufacturing and logistics facilities or through shortages in supply or labor (Rose, 2004; Jonkman et al., 2008). This can halt or slow production, thus reducing SC performance. To address supply-related disruptions, studies have proposed various solutions including the dual-sourcing procurement strategy, whereby manufacturers cooperate with two suppliers from different regions; increased warehousing and supply stockpiling; and cutting-edge digital technologies (Chopra, 2020). Cloud deployment, through which two or more firms are linked through information technology (IT) resources with shared information and funds (Lindner et al., 2010), is one of the digital technologies that is increasingly applied in SCs (Ellis et al., 2017).

After adopting cloud-based commerce networks, SC firms can enhance their performance by instantaneously exchanging real-time data and improving product availability (Toka et al., 2013; Chambers, 2020). Many pharmaceutical companies, such as Pfizer, have

* Corresponding author.
E-mail addresses: lmchen@nccu.edu.tw (L.-M. Chen), wlchang@ntut.edu.tw (W.-L. Chang).

https://doi.org/10.1016/j.tre.2021.102347
Received 13 September 2020; Received in revised form 19 April 2021; Accepted 19 April 2021
Available online 28 May 2021

moved their SC operations to the cloud; this enables their SC partners to plan and control material flows by accessing up-to-date, centralized data regarding shipments, arrival times, and the locations of dispatched products (Maziliauskaite, 2015; Jacques, 2016). Moreover, cloud deployment in SCs enhances SC resilience (Ivanov et al., 2019). For instance, when supply-related disruptions hit an upstream supplier, rather than frantically scrambling at the last minute, the cloud helps downstream SC partners to mitigate damages by quickly identifying upcoming threats, thus providing downstream firms with more time to prepare contingency measures. This resilience, which is attributable to enhanced SC visibility through the cloud, reduces the negative impacts of supply-related disruptions on SC firms' performance.

Given the benefits of cloud deployment for SC performance, an increasing number of firms have moved their SC activities to the cloud. However, these firms face a new disruption risk in the form of cyber-related disruptions, which are primarily caused by cyberattacks. The IT resources for computing and storage available through cloud-based platforms are based on a multitenant environment, under which a single cloud provider gives IT resources to firms inside and outside of the SC. Thus, hackers may attack platform members and their SC partners. In 2017, the notorious hacking group Red Apollo launched one of the largest cyber espionage campaigns by spreading spyware to many firms' IT systems through cloud service providers (Bond, 2018). This cyberattack resulted in the theft of data from many firms executing SC activities through their cloud service providers' IT platforms. Such cyber-related disruptions cause the loss of intangible capabilities such as reputation and public trust as well as reduce SC performance (Forbes Insights, 2014; Deloitte, 2014; Ismail, 2018).

Thus, under the cloud environment, SC firms face both supply- and cyber-related disruptions. These disruptions may become more frequent and unpredictable, leaving many managers unprepared. For example, no SC firm has predicted the risk of supply disruption due to workers being barred from work because of shelter-in-place orders during the coronavirus pandemic. Moreover, cyber criminals continually search for weak points in SCs to circumvent protection against cloud threats. Many people refer to these unpredictable events, such as the coronavirus pandemic and cyberattacks, as black swan events. Black swan events are generally absent from the mitigation plans developed by firms because they are outside the realm of immediate possibility; this leaves SC firms vulnerable to supply disruptions and cyberattacks. Therefore, it is urgent that SC firms explore *reactive* plans through which they can expend resources (e.g., money) to recover from disruptions. When recovering from supply- and cyber-related disruptions, some SC firms invest considerable resources to expedite their recovery. However, fast recovery may be suboptimal if their SC partners remain influenced by supply- or cyber-related disruptions. By contrast, other SC firms gradually expend resources to slowly recover from disruptions. This study aims to determine the best *recovery speeds* for SC firms that employ the cloud when recovering from supply- and cyber-related disruptions. The best recovery speeds were evaluated based on the firm's SC performance, which was measured by two capabilities: operational (e.g., production capacity and labor supply) and intangible (e.g., reputation, brand image, and public trust). A firm's operational capabilities are negatively affected by supply-related disruptions; thus, when a disruption occurs, these capabilities are downgraded. Similarly, a firm's intangible capabilities are negatively affected by cyber-related disruptions. After disruptions, the firm recovers the operational and intangible capabilities by consuming resources. The firm's recovery-speed choice affects the needed resources, the level of capability restoration, and SC performance.

To investigate firm recovery speeds, we developed a cellular automata (CA) model–a simulation model based on a grid in which each cell represents an SC firm. This grid structure can characterize the interdependencies between SC partners in a complex SC system (Ritter, 1999; Wu and Choi, 2005; Choi and Wu, 2009; Nair et al., 2009). In practice, a firm's SC performance depends not just on its operational capabilities but also on the operational capabilities of its immediate upstream and downstream neighbors. Material flow refers to the direct movement of goods between two directly related firms, and flow smoothness thus depends on the operational capabilities of a firm and its immediate neighbors. Therefore, to explore the impact of the operational capabilities of a firm and its immediate neighbors to this firm's SC performance and given that this firm's immediate neighbors cannot be replaced by other SC partners, the CA model which describes a firm's relationships with its immediate neighbors in a grid form is suitable. Notably, this CA model is a simplification of the common agent-based model in which neighbors are changeable, and it takes advantage of the reduction in computational complexity to simulate the dynamics of complex SCs facing disruptions (Nair et al., 2009).

The proposed CA model describes a two-dimensional networked cloud SC comprising multiple parallel chains in which SC partners from the same parallel chain exchange material and information using the same cloud provider. In the networked structure, the operational capabilities of a firm and its immediate neighbors directly influence its SC performance. In addition, cloud deployment complements an SC firm's operational capabilities by enhancing its intangible capabilities and thus improving SC performance. The aforementioned setting is consistent with the framework proposed by Rai et al. (2006), according to which IT-related capabilities enable a firm to strengthen its process integration capability and improve its SC performance.

On the basis of this context, the present study focused on three research questions:

1. What is the best speed for a cloud SC firm to recover from supply-related disruptions?
2. What is the best speed for a cloud SC firm to recover from cyber-related disruptions?
3. What is the impact of cloud deployment on the speed of an SC firm's recovery from supply-related disruptions?

The remainder of this paper is organized as follows. Section 2 reviews the relevant literature. Section 3 introduces the CA model, which was designed to investigate an SC firm's best recovery speeds from supply- and cyber-related disruptions. Next, Section 4 lists the simulation results, and Section 5 provides managerial implications. Finally, in Section 6, the conclusion is provided, and future research directions are suggested.

2. Literature review

This literature review examines three streams. First, we review studies that address the impact of information and digital technologies, including cloud deployment, on SCs. Second, we review studies related to the strategies used to deal with supply- and cyber-related disruptions. Specifically, we classify studies according to their strategies (i.e., proactive and reactive). Third, we review studies that use simulation techniques to investigate SCs under disruption risks.

2.1. Impact of IT and cloud deployment on SCs

IT systems have positive effects on the operational and SC performance of firms (Ivanov et al., 2019). Bharadwaj (2000) highlighted that the adoption of IT can benefit a firm's profitability. Similarly, Melville et al. (2004) found that IT augments a firm's organizational capabilities and facilitates business performance. Chen and Paulraj (2004) noted that IT can enhance SC collaboration capabilities by providing real-time information sharing among SC partners regarding demand forecasts, product availability, inventory levels, shipment status, and production requirements. Rai et al. (2006) indicated that IT enables firms to improve their SC integration capabilities, resulting in significant operational improvements. Moreover, Yu et al. (2018) showed that an IT-driven SC strengthens a firm's SC capabilities and thus benefits its financial performance. Recently, disruptive technologies, such as cloud computing, artificial intelligence, the Internet of things, and blockchain, have played key roles in driving SC innovation and in enhancing a firm's competitiveness and SC performance (Dutta et al., 2020; Li et al., 2020; Li, 2020; Van Nguyen et al., 2020; Wang et al., 2020; Liu et al., 2021; Niu et al., 2021).

In particular, the benefit of using cloud technology for SC management has been highlighted in several studies. Bruque-Cámara et al. (2016) revealed that cloud deployment helps the integration of SC information and material flows, thus positively influencing firms' SC performance. Moreover, Ireland and Webb (2007) and Wu et al. (2013) have demonstrated that cloud technology can strengthen interorganizational relationships between SC partners by increasing trust. However, the introduction of the cloud to SCs also presents cyber-related disruption risks. Marston et al., (2011), Godfrey and Zulkernine (2014), Levitin et al. (2018), and Gwebu et al. (2018) have shown that after cyberattacks, SC firms sustain losses in intangible capabilities such as trust and reputation. This reviewed studies revealed that cloud technology can have both positive and negative effects on conventional SCs. However, few studies have investigated the pros and cons of cloud adoption and then have quantitatively studied the corresponding impacts on firm SC performance. This study aims to fill this research gap by applying a simulation model.

2.2. Mitigation and recovery strategies under disruption risks

In this review, the definition of SC resilience is addressed, which has become an important topic in SC management because it complements conventional risk management processes (Fiksel et al., 2015). Sheffi (2005), Sheffi and Rice (2005), Sodhi and Lee (2007), Ritchie and Brindley (2007), Ponomarov and Holcomb (2009), and Kamalahmadi and Parast (2016) have commented that SC resilience can be described as the proactive capabilities of a firm (or an SC), namely preparation for and thus mitigation of disruptions. Moreover, SC resilience can be regarded as reactive capabilities, namely those that help the firm (or SC) recover from disruptions. Consequently, we first review studies introducing proactive strategies to manage supply- and cyber-related disruptions and then review studies of reactive strategies.

Numerous studies have proposed proactive methods to address supply-related disruption risks. For risks that might occur during production or sourcing, Torabi et al. (2015) discussed strategies, including the establishment of contracts with backup suppliers and the consideration of suppliers' business continuity plans, to enhance the resilience level of the supply base. They proposed a bi-objective, mixed-possibilistic, two-stage stochastic programming model to determine the optimal supplier selection and order allocation. Ivanov et al. (2016) considered a multistage SC problem and investigated the use of backup suppliers and capacity expansion during the planning stage for disruption risks. For each strategy, the authors assessed the service level performance and cost. Namdar et al. (2018) formulated a two-stage, stochastic, mixed-integer model to investigate resilient sourcing strategies, including single and multiple sourcing, backup-supplier contracts, spot purchasing, and collaboration and visibility. They found that the optimal resilience strategy depended on the risk-aversion level and the type of disruption. Specifically, single-sourcing and multiple-sourcing strategies had equal performance under low- and medium-risk aversion, but multiple sourcing was preferable to single sourcing under low-impact and high-frequency disruption risks. Petrovic and Kalata (2019) presented a multi-objective optimization model for supplier selection and order allocation based on the minimization of the supplier's risk (e.g., uncertainty in supply lead times and nonconformance rates of delivered components).

In addition to disruption risks during production and sourcing, some studies have focused on disruption risks in transportation and logistics. Wang et al. (2018) considered shipment insurance in express logistics and airline transportation as a proactive strategy to mitigate transportation disruptions. The authors proposed a Stackelberg game to study the interactions between the express logistics provider and its customers, and they used this game to determine the optimal insurance premiums. Veneti et al. (2017) addressed the shipping routing problem and proposed a time-dependent, bi-objective shortest path algorithm. The objective in their study was to minimize fuel consumption and the risk of a disrupted shipping route. Jafarian et al. (2019) investigated the inventory and routing problem by developing meta-heuristic approaches in which vehicle failure or breakdown was considered a potential disruption in a transportation system. They contributed to the decisions on order delivery times, the delivery volumes for each customer, and the routing sequence of customer visits during each period. The objective was to minimize the total transport and inventory costs while meeting customer demands. Siddiqui and Verma (2015) addressed transportation risk and operating cost in the routing and scheduling

problem for crude oil tankers by proposing a mixed-integer bi-objective optimization program. They showed that the shortest and cheapest routes may not minimize risk, because the cost-saving may not compensate for the cost increase caused by transportation disruptions. In addition, using large vessels to transport crude oil is the optimum scheduling solution if risk is a crucial concern, because this enables better exploitation of the economies of both cost and risk.

Strategies to mitigate cyber-related disruption risks in the cloud environment are detailed as follows. Some studies have proposed methods for identifying potential cloud risks before they occur. For example, Roumani and Nwankpa (2019) developed a hybrid model that employs machine learning and time-series methods to forecast cloud incidents. The results of this hybrid model can provide valuable information to IT managers, including information on incident regularity; managers can then utilize the information when deciding the techniques to implement for future incidents. Akinrolabu et al. (2019) developed a novel cloud risk assessment model called Cyber Supply Chain Cloud Risk Assessment. The model included a systematic analysis of cloud risks, a visual representation of the cloud SC, and an assessment of the cybersecurity posture of cloud service suppliers. Their results can help IT managers to identify cloud vulnerabilities and threats and to improve their defenses against risks.

In addition to proactive strategies for mitigating disruption risks, we also review studies that explore strategies for recovery after disruptions in production, sourcing, or transportation. Paul et al. (2014) developed a disruption-recovery model for a two-stage production-inventory system. They applied a new approach to obtain the recovery plan, in which the optimal batch size after the disruption was determined on a real-time basis. Hishamuddin et al. (2012) and Hishamuddin et al. (2013) have considered transportation disruption risks and have developed a disruption-recovery model for the production-inventory system. They have solved this model by using an efficient heuristic to determine the optimal order and production quantity during a recovery window. Mu et al. (2011) developed Tabu Search algorithms to solve the disrupted vehicle routing problem, in which a vehicle breaks down during the delivery; the recovery strategy for this transportation disruption relies on the generation of a new routing solution with minimized costs. Ivanov et al. (2017) reviewed studies on disruption recovery and classified quantitative methods in terms of disruption risks and recovery measures.

Other papers have explored *ex ante* and *ex post* disruptions by investigating proactive and recovery strategies. Hu et al. (2013) discussed the problem in which a firm (buyer) uses price and order quantity incentives to encourage the supplier to make investments for restoration based on two cases: when the firm commits to the incentive *ex ante* (before the disruption) and when it commits *ex post* (after the disruption). Sawik (2017) proposed a mixed-integer programming method to select a supply portfolio under disruption risk; the proposed portfolio approach combined decisions made before, during, and after disruptions. Khalili et al. (2017) presented a two-stage, scenario-based mixed stochastic-possibilistic model for an integrated production and distribution planning problem. In the first stage of their model, proactive risk-mitigation decisions are determined, and the second stage specifies recovery plans for lost capacities (e.g., additional capacity in production facilities, backup routes for transportation links, and emergency inventory). Goldbeck et al. (2020) presented a novel multistage stochastic programming model that is used to optimize pre-disruption investment decisions regarding the capacity and repair capability of production and logistics systems under the risk of damage; their model also optimizes the post-disruption dynamic adjustment of SC operations and the allocation of repair resources. Bier et al. (2020), Duong and Chong (2020), Xu et al. (2020), Choi (2021), and Chowdhury et al. (2021) have provided a comprehensive overview of the current methods for mitigating and recovering from disruptions in SCs, transportation, and logistics.

Some papers have addressed reactive methods against cyber-related disruptions in the e-health domain (Sahi et al., 2016; Qi et al., 2017). For example, Sahi et al. (2016) discussed disaster recovery plans to guarantee the availability and continuity of e-health systems during a disaster (the recovery plan enables data owners and patients to have complete and safe control over their records). However, in the cloud SC domain, most studies related to cyber damage have focused on proactive strategies. Thus, the present study fills this research gap.

In summary, the reviewed studies have mainly focused on strategies to mitigate or recover from supply- and cyber-related disruptions. By contrast, the present study investigated the speeds of recovery from disruptions. To the best of our knowledge, no quantitative research has been conducted on this topic.

2.3. Simulation techniques

Various studies have applied simulation techniques to study SCs under disruption risks. Simulation is a suitable technique when mathematical modeling is too expensive for complex SC systems (Pathak et al., 2007). Wilson (2007) considered a vendor-managed system under transportation disruption risks by simulating a five-echelon SC problem and compared the proposed vendor-managed inventory system with the conventional inventory system. Ivanov (2019) studied a contingent recovery policy following disruptions through a discrete-event simulation. Tan et al., (2020) implemented a discrete-event simulation by considering the post-disruption recovery time and costs; from the results, they identified the appropriate mitigation and contingency strategies to improve SC resilience. Ivanov (2020) conducted a discrete-event simulation of the 2020 COVID-19 pandemic to examine the impact of disruption durations and their ripple effects. Ivanov and Dolgui (2020) proposed a data-driven simulation model for managing disruption risks; SCs with actual transportation, inventory, demand, and capacity data enable decision-making regarding proactive resilient SC design and reactive real-time disruption risk management. The authors contributed to reveal relationships among risk data, disruption modeling, and performance assessment. Besides, agent-based simulation is another popular technique, and it is relevant to the CA model used in the present study. Li and Chan (2013) proposed an agent-based model to simulate make-to-order and make-to-stock SCs with a dynamic structure. Hou et al. (2018) used an agent-based model to analyze the impact of trust on the topology of SC networks and SC resilience under disruption risks. They demonstrated that firms adopting the trust-based rule are the most resilient in the face of disruptions. Nair and Vidal (2011) used the agent-based model to examine the relationship between the topology of a supply

network and its robustness given random failure and targeted attacks. They suggested that to ensure resilience, SCs should balance the advantages of a clustered SC facilities with its potential disadvantages when disruptions occur. Zhao et al. (2019) developed an agent-based model to investigate two adaptive strategies against disruptions employed by SC firms: a reactive strategy that restructures the network after disruptions affect first-tier suppliers and a proactive strategy implemented when a distant disruption is observed but has not yet impacted the focal firms. They further discussed the improvement of resilience against disruptions by leveraging these adaptive strategies.

In contrast to the common agent-based models, in which each SC firm typically determines its individual rules from a specific set, the present study simulated a case in which all SC firms follow the same rules (i.e., the same recovery speed) under supply- or cyber-related disruptions; moreover, a firm's SC performance is directly affected by its immediate upstream and downstream partners, which are fixed because material flows are directly connected. Thus, we developed a CA simulation model in which all SC firms adopt the same recovery speed and in which an SC firm's immediate neighbors remain unchanged. Nair et al. (2009) and Chen et al. (2015) have used the CA model to explore decision-making for an entire SC system (rather than for the individual decisions of SC firms), and they used this to reveal the dependencies between immediate neighbors. To the best of our knowledge, the present study is first to apply the CA model to cloud SCs under both supply- and cyber-related disruptions.

In summary, this study contributes to the literature on SC and logistics management as follows. First, we explored the best recovery speeds for cloud SCs when firms face supply- and cyber-related disruptions. Second, we developed a CA model to explore the effects of the operational and intangible capabilities of a cloud SC firm on its SC performance. Among the studies investigating disruptions by using simulation models, none have used this CA model to discuss recovery speeds in the cloud SC. These novel contributions complement existing research in SC management.

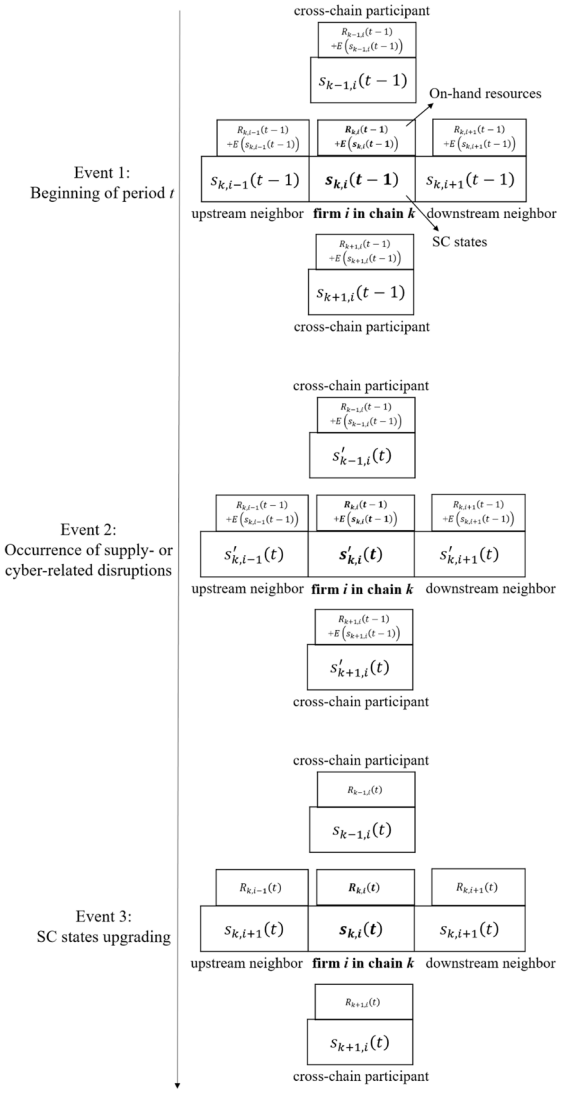

Fig. 1. Dynamics of a firm's SC states and its on-hand resources.

3. CA model

The CA model is designed to simulate the dynamics of the networked cloud SC for T periods. This networked structure comprises three one-dimensional chains arranged in parallel, indexed by the chain $k = \{1, 2, 3\}$. Each of these one-dimensional chains includes N firms, labeled as $1, 2, \cdots, N$. Thus, the CA model forms a two-dimensional grid, with each cell's neighborhood as a *von Neumann neighborhood* (Fig. 1) and each SC firm having four neighbors: the immediate upstream partner (the left neighbor), the immediate downstream partner (the right neighbor), and two competing neighbors (cross-chain participants). For example, SC firm i in chain k has one upstream neighbor (firm $i-1$ in chain k), one downstream neighbor (firm $i+1$ in chain k), and two cross-chain participants (firms i in chain $k-1$ and i in chain $k+1$).

The operational capabilities of firm i in chain k (e.g., production capacity and labor supply) in period t are represented by the operational state $x_{k,i}(t)$, which has three levels: 0 (low), 1 (medium), and 2 (high); thus, $x_{k,i}(t) \in \{0, 1, 2\}$. Chen et al. (2015) also classified the operational capabilities of a firm into three levels. Similarly, its intangible capabilities (e.g., reputation, brand image, and public trust) are represented by the intangibles state $y_{k,i}(t)$, which also has three levels: 0 (low), 1 (medium), and 2 (high); thus, $y_{k,i}(t) \in \{0, 1, 2\}$. The capability levels (for operational or intangible capabilities) are based on the firm's maximum capabilities. That is, each level is assigned an equal one-third proportion. For instance, when a firm's operational capabilities are at 20%, its operational state is classified as 0 (i.e., low). Based on these settings, simulation is conducted to describe the SC capabilities of firm i during period t based on its SC states $s_{k,i}(t)$, where $s_{k,i}(t) = \left(x_{k,i}(t), y_{k,i}(t)\right)$ has 3×3 combinations.

Other assumptions used in this CA model are clarified as follows. First, an SC firm in a one-dimensional chain cannot be an SC partner in another chain. Second, the dynamics (i.e., changes in the SC states) of an SC firm are assumed to be discrete (Robertson and Caldart, 2009). Third, a firm's SC performance in a given period is related to its SC states in this period, and we describe it as resource acquisition. Furthermore, we interpret a firm's SC performance from the beginning of the simulation to the current period based on its cumulative resources. Fourth, an SC firm's operational and intangibles states, which form the SC states, are assumed to have an additive effect on resource acquisition during a period. Finally, when disruptions occur, a firm's cumulative resources are expended for recovery.

3.1. Dynamics in SC states

In this subsection, we detail the effects of supply- and cyber-related disruptions on a firm's SC states and explain how the CA model describes the recovery process based on three time events (Fig. 1): the beginning of period t (Event 1), the occurrence of supply- or cyber-related disruptions (Event 2), and the SC states upgrading (Event 3).

Beginning of period *t*: At the beginning of period t, firm i in chain k gains resources $E\left(s_{k,i}(t-1)\right)$ subject to its SC states in the previous period. As mentioned in the assumptions, resource acquisition is based on gains from operational capabilities and gains from intangible capabilities. We define

$$E_x(t-1) = \begin{cases} r_x^0, & \text{if } \min\left(x_{k,i-1}(t-1), x_{k,i}(t-1), x_{k,i+1}(t-1)\right) = 0 \\ r_x^1, & \text{if } \min\left(x_{k,i-1}(t-1), x_{k,i}(t-1), x_{k,i+1}(t-1)\right) = 1 \\ r_x^2, & \text{if } \min\left(x_{k,i-1}(t-1), x_{k,i}(t-1), x_{k,i+1}(t-1)\right) = 2 \end{cases} \tag{1}$$

to capture resource acquisition based on operational capabilities, which are related to the operational capabilities of immediate SC neighbors. This result can be explained as follows. When either of a firm's upstream or downstream SC neighbor is in a low operational state, the physical flow of commodities becomes unreliable. Thus, even if firm i has a higher operational state, it may not have high SC performance and it thus acquires fewer resources from the previous period. Resource acquisition also relies on intangible capabilities (Ireland and Webb, 2007; Hou et al., 2018) as follows:

$$E_y(t-1) = \begin{cases} r_y^0, \textit{if } \ y_{k,i}(t-1) = 0 \\ r_y^1, \textit{if } \ y_{k,i}(t-1) = 1 \\ r_y^2, \text{if } \ y_{k,i}(t-1) = 2 \end{cases} \tag{2}$$

In summary, from Eqs. (1) and (2), the additive effect of operational and intangibles states results in the following resource acquisition in period t:

$$E\left(s_{k,i}(t-1)\right) = E_x(t-1) + E_y(t-1). \tag{3}$$

Moreover, the resources accumulated from the beginning of the simulation to period t is

$$E\left(s_{k,i}(t-1)\right) + R_{k,i}(t-1), \tag{4}$$

where $R_{k,i}(t-1)$ is the total on-hand resources at the end of period $t-1$.

Occurrence of supply- or cyber-related disruptions: When supply- or cyber-related disruptions occur in period t, a firm's operational or intangibles states are reduced; however, the level of decrease varies depending on the severity of the disruption (Cheng

et al., 2020). When firm i experiences supply-related disruptions and thus faces a slight loss in operational capabilities in period t, its operational state is expressed as $x'_{k,i}(t) = \max\{x_{k,i}(t-1) - 1, 0\}$; however, if the loss in operational capabilities is severe, its operational state decreases to $x'_{k,i}(t) = 0$. Similarly, when cyber-related disruption causes a slight loss in intangible assets, the intangibles state of firm i is reduced to $y'_{k,i}(t) = \max\{y_{k,i}(t-1) - 1, 0\}$; however, if the loss is severe, then its intangibles state decreases to $y'_{k,i}(t) = 0$. This firm's post-disruption SC states are denoted by $s'_{k,i}(t) = \left(x'_{k,i}(t), y'_{k,i}(t)\right)$

SC states upgrading: To recover from losses in operational or intangible capabilities, firm i in chain k must consume resources, so that its SC states can return from $s'_{k,i}(t) = \left(x'_{k,i}(t), y'_{k,i}(t)\right)$ to the target states $\hat{s}_{k,i}(t) = \left(\hat{x}_{k,i}(t), \hat{y}_{k,i}(t)\right)$, where $\hat{x}_{k,i}(t) \geq x'_{k,i}(t)$ and $\hat{y}_{k,i}(t) \geq y'_{k,i}(t)$. Notably, changes in states are viewed from the behavioral operations perspective (Gintis, 2000; Chen et al., 2015; Fahimnia et al., 2019), and these changes can be used to reflect a firm's recovery speed following a disruption. An upgrade to a firm's SC states through resource consumption is expressed as follows:

$$C_u(t) = \begin{cases} c_u^{01} & \text{for } u'_{k,i}(t) = 0 \text{ and } \hat{u}_{k,i}(t) = 1 \\ c_u^{12} & \text{for } u'_{k,i}(t) = 1 \text{ and } \hat{u}_{k,i}(t) = 2 \\ c_u^{02} & \text{for } u'_{k,i}(t) = 0 \text{ and } \hat{u}_{k,i}(t) = 2 \end{cases}, \tag{5}$$

where $u \in \{x, y\}$. In particular, $C_x(t)$ represents the resources needed to upgrade the operational state, and $C_y(t)$ denotes the resources needed to upgrade the intangibles state. Thus, the total resources needed to upgrade the SC states of firm i in chain k from $s'_{k,i}(t)$ to $\hat{s}_{k,i}(t)$ are

$$C\left(s'_{k,i}(t), \hat{s}_{k,i}(t)\right) = C_x(t) + C_y(t). \tag{6}$$

However, on-hand resources may be inadequate to achieve the target SC states. For example, when resources are initially used to meet the target operational state, but the remaining resources are insufficient to reach the target intangibles state, the firm cannot improve its intangible capabilities. Accordingly, we consider two resource consumption principles: prioritizing the firm's resource consumption for 'loss of operational capabilities' over 'loss of intangible capabilities', called the *resource consumption principle* Δ^P, and prioritizing the resources for 'loss of intangible capabilities' over 'loss of operational capabilities', called the *resource consumption principle* Δ^C. Based on these two resource consumption principles and the possibility that resources may be insufficient to upgrade a firm's SC states to the target SC states, there are five cases to illustrate updates to the SC states of firm i in chain k at the end of period t, $s_{k,i}(t) = \left(x_{k,i}(t), y_{k,i}(t)\right)$:

Case 1: If this firm has sufficient on-hand resources to meet its target SC states, then the operational and intangibles states are increased to the target values (i.e., $s_{k,i}(t) = \hat{s}_{k,i}(t)$, $x_{k,i}(t) = \hat{x}_{k,i}(t)$, and $y_{k,i}(t) = \hat{y}_{k,i}(t)$).
Case 2: If the resources are sufficient to meet the target intangibles state but insufficient to meet the target operational state, then the operational state is maintained (i.e., $x_{k,i}(t) = x'_{k,i}(t)$), and the intangibles state is upgraded to the target value (i.e., $y_{k,i}(t) = \hat{y}_{k,i}(t)$).
Case 3: If the resources are sufficient to meet the target operational state but insufficient to meet the target intangibles state, then the operational state is upgraded to the target value (i.e., $x_{k,i}(t) = \hat{x}_{k,i}(t)$), and the intangibles state is maintained (i.e., $y_{k,i}(t) = y'_{k,i}(t)$).
Case 4: Assume that the resources are sufficient to meet either the target operational state or the target intangibles state but not both; then, under Δ^P, the operational state is upgraded to the target value (i.e., $x_{k,i}(t) = \hat{x}_{k,i}(t)$), and the intangibles state is maintained (i.e., $y_{k,i}(t) = y'_{k,i}(t)$); under Δ^C, the operational state is maintained (i.e., $x_{k,i}(t) = x'_{k,i}(t)$), and the intangibles state is upgraded to the target value (i.e., $y_{k,i}(t) = \hat{y}_{k,i}(t)$).
Case 5: If this firm has inadequate resources to meet the target operational and intangibles states, then both states are maintained (i.e., $s_{k,i}(t) = s'_{k,i}(t)$, $x_{k,i}(t) = x'_{k,i}(t)$, and $y_{k,i}(t) = y'_{k,i}(t)$).

Based on these cases and Eqs. (3) to (6), the SC states of firm i in chain k at the end of period t can be represented as follows:

$$s_{k,i}(t)=\begin{cases}\widehat{s}_{k,i}(t) & \text{for } R_{k,i}(t-1)+E\left(s_{k,i}(t-1)\right)\geq C\left(s_{k,i}^{'}(t),\widehat{s}_{k,i}(t)\right)\\ \left(x_{k,i}^{'}(t),\widehat{y}_{k,i}(t)\right) & \text{for } C_x(t)>R_{k,i}(t-1)+E\left(s_{k,i}(t-1)\right)\geq C_y(t)\\ \left(\widehat{x}_{k,i}(t),y_{k,i}^{'}(t)\right) & \text{for } C_y(t)>R_{k,i}(t-1)+E\left(s_{k,i}(t-1)\right)\geq C_x(t)\\ \begin{pmatrix}\left(\widehat{x}_{k,i}(t),y_{k,i}^{'}(t)\right)\ \text{under}\ \Delta^P;\\ \left(x_{k,i}^{'}(t),\widehat{y}_{k,i}(t)\right)\ \text{under}\ \Delta^C\end{pmatrix} & \text{for } C\left(s_{k,i}^{'}(t),\widehat{s}_{k,i}(t)\right)>R_{k,i}(t-1)+E\left(s_{k,i}(t-1)\right)\geq\max\left(C_x(t),C_y(t)\right)\\ s_{k,i}^{'}(t) & \text{otherwise}\end{cases}.$$

In addition, this firm's on-hand resources at the end of period t is updated as follows:

$$R_{k,i}(t)=\begin{cases}R_{k,i}(t-1)+E\left(s_{k,i}(t-1)\right)-C\left(s_{k,i}^{'}(t),\widehat{s}_{k,i}(t)\right) & \text{for } R_{k,i}(t-1)+E\left(s_{k,i}(t-1)\right)\geq C\left(s_{k,i}^{'}(t),\widehat{s}_{k,i}(t)\right)\\ R_{k,i}(t-1)+E\left(s_{k,i}(t-1)\right)-C_y(t) & \text{for } C_x(t)>R_{k,i}(t-1)+E\left(s_{k,i}(t-1)\right)\geq C_y(t)\\ R_{k,i}(t-1)+E\left(s_{k,i}(t-1)\right)-C_x(t) & \text{for } C_y(t)>R_{k,i}(t-1)+E\left(s_{k,i}(t-1)\right)\geq C_x(t)\\ R_{k,i}(t-1)+E\left(s_{k,i}(t-1)\right)-I(t) & \text{for } C\left(s_{k,i}^{'}(t),\widehat{s}_{k,i}(t)\right)>R_{k,i}(t-1)+E\left(s_{k,i}(t-1)\right)\\ R_{k,i}(t-1)+E\left(s_{k,i}(t-1)\right) & \geq\max\left(C_x(t),C_y(t)\right)\\ & \text{otherwise}\end{cases},$$

Table 1
Recovery speeds.

Recovery-speed choices from supply-related disruptions (SRDs)	
Radical SRD-1	$x_{k,i}(t)=2$
Incremental SRD-2	$x_{k,i}(t)=\min\left\{x_{k,i}^{'}(t)+1,2\right\}$
Relaxed benchmarking SRD-3	If at least one of the immediate neighbors' operational state or its operational state is 2, $x_{k,i}(t)=2$; otherwise, $x_{k,i}(t)=1$.
Rigorous benchmarking SRD-4	If at least two of the immediate operational states or its operational state is 2, $x_{k,i}(t)=2$; otherwise, $x_{k,i}(t)=1$.
Matching SRD-5	$x_{k,i}(t)=\max\left\{x_{k,i-1}^{'}(t),x_{k,i}^{'}(t),x_{k,i+1}^{'}(t),x_{k-1,i}^{'}(t),x_{k+1,i}^{'}(t)\right\}$
Market-driven (from its downstream neighbor and cross-chain participants) SRD-6	If $x_{k,i}^{'}(t)<\max\left\{x_{k,i-1}^{'}(t),x_{k-1,i}^{'}(t),x_{k+1,i}^{'}(t)\right\}$, $x_{k,i}(t)=\max\left\{x_{k,i-1}^{'}(t),x_{k-1,i}^{'}(t),x_{k+1,i}^{'}(t)\right\}$; otherwise, $x_{k,i}(t)=\min\left\{x_{k,i}^{'}(t)+1,2\right\}$.
Market-driven (from its upstream neighbor and cross-chain participants) SRD-7	If $x_{k,i}^{'}(t)<\max\left\{x_{k,i+1}^{'}(t),x_{k-1,i}^{'}(t),x_{k+1,i}^{'}(t)\right\}$, $x_{k,i}(t)=\max\left\{x_{k,i+1}^{'}(t),x_{k-1,i}^{'}(t),x_{k+1,i}^{'}(t)\right\}$; otherwise, $x_{k,i}(t)=\min\left\{x_{k,i}^{'}(t)+1,2\right\}$.
Market-driven (from its up- and down-stream neighbors and cross-chain participants) SRD-8	If $x_{k,i}^{'}(t)<\max\left\{x_{k,i-1}^{'}(t),x_{k,i+1}^{'}(t),x_{k-1,i}^{'}(t),x_{k+1,i}^{'}(t)\right\}$, $x_{k,i}(t)=\max\left\{x_{k,i-1}^{'}(t),x_{k,i+1}^{'}(t),x_{k-1,i}^{'}(t),x_{k+1,i}^{'}(t)\right\}$; otherwise, $x_{k,i}(t)=\min\left\{x_{k,i}^{'}(t)+1,2\right\}$.
Recovery-speed choices from cyber-related disruptions (CRDs)	
Radical CRD-1	$y_{k,i}(t)=2$
Progressive CRD-2	$y_{k,i}(t)=\min\left\{y_{k,i}^{'}(t-1)+1,2\right\}$
Relaxed benchmarking CRD-3	If at least one of the immediate neighbors' intangibles state or its intangibles state is 2, $y_{k,i}(t)=2$; otherwise, $y_{k,i}(t)=1$.
Rigorous benchmarking CRD-4	If at least two of the immediate intangibles states or its intangibles state is 2, $y_{k,i}(t)=2$; otherwise, $y_{k,i}(t)=1$.
Matching CRD-5	$y_{k,i}(t)=\max\left\{y_{k,i}^{'}(t),y_{k-1,i}^{'}(t),y_{k+1,i}^{'}(t)\right\}$
Market-driven CRD-6	If $y_{k,i}^{'}(t)<\max\left\{y_{k-1,i}^{'}(t),y_{k+1,i}^{'}(t)\right\}$, $y_{k,i}(t)=\max\left\{y_{k-1,i}^{'}(t),y_{k+1,i}^{'}(t)\right\}$; otherwise, $y_{k,i}(t)=\min\left\{y_{k,i}^{'}(t)+1,2\right\}$.

where $I(t) = \begin{cases} C_x(t), under\ \Delta^P \\ C_y(t), under\ \Delta^C \end{cases}$.

Notably, when supply-related disruptions do not hit in period t, the firm does not consume on-hand resources so that $x_{k,i}(t) = x_{k,i}(t-1)$; that is, Events 2 and 3 are skipped for the update of its operational state. Similarly, $y_{k,i}(t) = y_{k,i}(t-1)$ when cyber-related disruptions do not occur in period t.

3.2. Recovery-speed choices

This subsection addresses the recovery-speed choices made by firms when upgrading their SC states from $s'_{k,i}(t)$ to $s_{k,i}(t)$. When implementing CA simulation, these choices are commonly referred to as the rules for updating an agent's state. Given that firm i in chain k has nine (3×3) possible SC states (i.e., three levels of the operational state and three levels of the intangibles state) and given that it can directly interact with its neighbors (i.e., upstream and downstream SC partners and two cross-chain participants), $59049 (= 9^5)$ possible scenarios dictate the SC states of the firm and its immediate neighbors following disruptions. For each scenario, we assign one of the nine possible SC states to the firm as its latest SC states when the firm is recovering from disruptions. This indicates that searching for the optimal movement of recovery from $s'_{k,i}(t)$ to $s_{k,i}(t)$ would be time-consuming and impractical. Thus, the CA model is adopted following the modeling practice applied in complex adaptive systems (Gintis, 2000; Miller and Page, 2009): we consider eight recovery speeds for supply-related disruptions (SRD-1 to SRD-8), which an SC firm can use to restore its lost operational capabilities, and six recovery speeds for cyber-related disruptions (CRD-1 to CRD-6), which the firm can use to regain intangibles such as reputation and public trust. These speeds are based on real-world decision-making, as shown in Table 1. In the SC network, firms located in different one-dimensional chains may not experience a simultaneous loss of intangible capabilities, because they might have different cloud services providers.

SRD-1 is referred to as the *radical* choice because each SC firm pursues a fast and full recovery by aggressively restoring its operational state to "high" (i.e., the highest level of operational capabilities) following any supply-related mild to severe disruptions. This choice is mostly adopted by large global companies because they have sufficient resources to immediately restore their full operational capabilities. SRD-2 is referred to as the *incremental* choice; following this option, an SC firm gradually repairs damages caused by supply-related disruptions. This choice is often used by small and medium enterprises because they generally lack additional resources (or capital) for recovery. For instance, following the 2011 earthquake and tsunami in Japan, small Japanese suppliers of NAND flash memory required an average of 6 months to regain their full production capacity (CNN, 2011). Because of the incremental upgrade of the firm's operational state, SRD-2 is a slower than SRD-1.

In the SRD-3 and SRD-4 recovery speeds, an SC firm benchmarks its immediate neighbors' operational capabilities. For example, after the 2011 earthquake and tsunami in Japan, suppliers of parts for Toyota that were severely affected obtained direct assistance from the Reinforce Supply Chain Under Emergency (RESCUE) database, which shared the information on Toyota suppliers (Forbes, 2016). This increased SC visibility enabled firms in Toyota's SCs to benchmark their immediate neighbors' operational capabilities. Accordingly, when a firm's immediate upstream and downstream neighbors have the highest level of operational capabilities, the firm is more likely to pursue a "high" operational state, because neighbors having equivalent operational capabilities can lead to smooth SC flows and can benefit the firm's SC performance. In particular, for SRD-3, which is referred to as the *relaxed benchmarking* speed, a firm facing supply-related disruptions returns to the "high" operational state when any of its immediate neighbors is in a "high" state; however, this firm remains in or moves to the "medium" state when its neighbors are not in the "high" state. For SRD-4, which is referred to as the *rigorous benchmarking* choice, an SC firm returns to the "high" operational state when at least two immediate neighbors are in "high" states; otherwise, it remains in or moves to the "medium" state.

SRD-5 is the *matching* choice; following this approach, an SC firm matches its operational state with the highest level of its immediate SC neighbors, but this occurs only if one of these neighbors is functioning at an operational level higher than that of the firm. Otherwise, it maintains its operational state. Following the 2011 floods in Thailand, many of Honda's parts suppliers adopted the matching approach to recover from supply-related disruptions because Honda's car assembly sites and many of its suppliers were all located in Ayutthsaya, which was the most flood-damaged area of Thailand. If a parts supplier had returned to its full operational capabilities after flood damage, SC performance would not have been optimized because other suppliers and Honda itself might not have recovered from the damage (Haraguchi and Lall, 2015). Consequently, the matching option was a suitable recovery speed for Honda's parts suppliers following the 2011 floods in Thailand.

SRD-6 to SRD-8, referred to as *market-driven* choices, are choices driven by market pressure; that is, an SC firm's immediate neighbors drive its recovery speed from supply-related disruptions. For example, when the disrupted firm cannot keep pace with its SC neighbors' flow of goods and services, it faces an increasing likelihood of being excluded from the SC, because it can slow down the entire SC. In SRD-6, an SC firm's downstream neighbor and its cross-chain participants stimulate its recovery from supply-related disruptions; thus, if this firm's downstream neighbor or any of its cross-chain participants has a better operational state, it upgrades its operational state to this level; otherwise, it incrementally rebuilds its operational capabilities. In SRD-7, an SC firm's upstream neighbor and its cross-chain participants drive its recovery; hence, if any of these firms have a higher operational state, it updates its operational state to match this level; otherwise, this firm incrementally rebuilds its operational capabilities. In SRD-8, an SC firm upgrades its operational state to the maximum operational state of all neighbors; otherwise, it incrementally rebuilds its operational capabilities.

Notably, the market-driven recovery speeds from supply-related disruptions (SRD-6, SRD-7, and SRD-8) encourage SC firms to independently achieve the "high" operational state (the highest level of operational capabilities) even if its neighbors are not at the

highest level. Therefore, these are faster speeds than the benchmarking recovery speeds (SRD-3 and SRD-4), in which the SC firm's operational state is independently increased to only a "medium" level. In addition, the matching choice (SRD-5) is the slowest recovery speed from supply-related disruptions.

The speeds of recovery from cyber-related disruptions are described as follows. CRD-1 is referred to as the *radical* choice; following this approach, an SC firm always chooses to regain the highest intangibles state. In other words, the underperforming firm returns to the "high" intangibles state regardless of the severity of its loss of intangible capabilities. In CRD-2, which is the *progressive* choice, the firm moves its intangibles state from "low" to "medium" or from "medium" to "high". Therefore, CRD-2 is a slower recovery speed than CRD-1. Because cyber disruptions are caused by a third party, namely the cloud service provider, all SC partners located in the same one-dimensional chain suffer the same loss of intangibles when cyber-related disruptions occur. Therefore, CRD-1 and CRD-2 are independent of the firm's all immediate neighbors (i.e., upstream and downstream firms and cross-chain participants). CRD-3 and CRD-4 are referred to as *benchmarking* recovery speeds; the firm benchmarks its immediate neighbors' intangibles states when they have the highest level of intangible capabilities. In CRD-5, which is the *matching* choice, the SC firm matches its intangibles state with the highest intangibles state of its immediate neighbors when one of these neighbors has a higher intangibles state. In CRD-6, which is the *market-driven* choice, the SC firm upgrades its intangibles state by matching with the maximum intangibles state of its cross-chain neighbors if any of them has a higher state; otherwise, it incrementally upgrades its intangibles state.

Among CRD-3 to CRD-6, CRD-5 is the slowest recovery speed. The market-driven recovery speed (CRD-6), which likely encourages an SC firm to independently achieve the "high" intangibles state, is faster than the two benchmarking recovery speeds (CRD-3 and CRD-4), in which the SC firm's intangibles state is independently upgraded to only "medium".

3.3. Parameter setting

The parameter settings used in the CA model are as follows (the base case). We set $N = 5$, $T = 180$, and $(f_x, g_x) = \left(\frac{17}{365}, \frac{50}{365}\right)$ based on the empirical dataset provided by Sheffi (2005) for the likelihood of "severe" and "mild" supply-related disruptions, where f is the severe case and g is the mild case; similarly, the likelihood of cyber-related disruptions is set as $\left(f_y, g_y\right) = \left(\frac{17}{365}, \frac{50}{365}\right)$. An SC firm's resource acquisition from its operational state at the beginning of period t, which is denoted by $E_x(t-1)$ $(r_x^0, r_x^1, \text{or}, r_x^2)$ in Eq. (1), is set with four scenarios (Table 2). $E_x(t-1)$ is measured by $\min\left(x_{k,i-1}(t-1), x_{k,i}(t-1), x_{k,i+1}(t-1)\right)$, and it can be equal to 0, 1, or 2. Similarly, we consider four scenarios for an SC firm's resource acquisition from its intangibles state, which is denoted by $E_y(t)$ $(r_y^0, r_y^1, \text{or}, r_y^2)$ in Eq. (2). $E_y(t)$ is measured by $y_{k,i}(t-1)$, which can be equal to 0, 1, or 2. Six scenarios are considered for $C_x(t)$ $(c_x^{01}, c_x^{12}, \text{or}, c_x^{02})$, which is the resources consumed to upgrade the SC firm's operational state, as illustrated in Eq. (5). Additionally, six scenarios are considered for $C_y(t)$ $(c_y^{01}, c_y^{12}, \text{or}, c_y^{02})$, which is those consumed to upgrade the intangibles state.

4. Simulation results

4.1. Base case and sensitivity analysis

The simulation results are presented as the means of 200 simulations. Tables 3–6 list the different combinations of recovery speeds following supply- and cyber-related disruptions; for each combination, the results comprised two parts: the average SC partner's SC performance (i.e., on-hand resources presented at the bottom of each cell) and the average SC states (presented in parentheses at the top of each cell). Numbers in bold with a gray background highlight the results with the best combinations of recovery speeds, where the SC firm achieves the highest SC performance or where its SC performance is within 5% of the highest SC performance.

For the base case (Table 3), the best speed for recovery from cyber-related disruptions is the matching speed (CRD-5). To recover from supply-related disruptions, three choices are excellent; from high to low SC performance, these choices were rigorous benchmarking (SRD-4), matching (SRD-5), and relaxed benchmarking (SRD-3).

In addition to the base case, we perform sensitivity analysis for a cloud SC firm's recovery based on various parameters (Montgomery, 1991). We consider three risk levels for supply-related disruptions $(f_x, g_x) = \left(\left(\frac{17}{365}, \frac{134}{365}\right), \left(\frac{17}{365}, \frac{50}{365}\right), \left(\frac{7}{365}, \frac{10}{365}\right)\right)$ (i.e., high to

Table 2
Resource acquisition and consumption scenarios.

Parameter description	Values
Resource acquisition: $\min\left(x_{k,i-1}(t-1), x_{k,i}(t-1), x_{k,i+1}(t-1)\right) = [0,1,2]$ $y_{k,i}(t-1) = [0,1,2]$	[0.5, 0.75, 1] [0.25, 0.5, 0.75] [0.5, 1, 1.5] [0.25, 0.375, 0.4375]
Resource consumption: $C_x(t) = [0 \to 1, 1 \to 2, 0 \to 2]$ $C_y(t) = [0 \to 1, 1 \to 2, 0 \to 2]$	[1, 5, 9] [1, 10, 22] [2, 5, 7] [5, 1, 6] [10, 1 11] [5, 2, 7]

Table 3
Base case.

Base case								
	SRD-1	SRD-2	SRD-3	SRD-4	SRD-5	SRD-6	SRD-7	SRD-8
CRD-1, Δ^P	(1.51,1.44)	(1.71,1.39)	(1.61,1.48)	(1.15,1.49)	(1.61,1.49)	(1.64,1.40)	(1.64,1.40)	(1.63,1.40)
CRD-3, Δ^P	63.96	62.34	69.60	73.83	69.98	63.67	63.68	63.76
CRD-4, Δ^P								
CRD-2, Δ^P	(1.40,1.67)	(1.69,1.58)	(1.54,1.67)	(1.11,1.65)	(1.53,1.69)	(1.58,1.61)	(1.58,1.61)	(1.56,1.62)
	63.38	61.99	69.66	72.77	70.12	63.09	63.10	63.15
CRD-5, Δ^P	(1.60,1.21)	(1.78,1.15)	**(1.69,1.24)**	**(1.20,1.29)**	**(1.69,1.24)**	(1.72,1.18)	(1.72,1.18)	(1.70,1.18)
	83.52	82.55	**92.00**	**96.19**	**92.29**	83.45	83.45	83.29
CRD-6, Δ^P	(1.45,1.62)	(1.70,1.55)	(1.56,1.64)	(1.14,1.63)	(1.56,1.65)	(1.61,1.57)	(1.61,1.58)	(1.59,1.58)
	63.72	62.22	69.67	73.53	69.89	63.48	63.58	63.47
CRD-1, Δ^C	(1.44,1.51)	(1.68,1.42)	(1.56,1.52)	(1.10,1.49)	(1.56,1.54)	(1.60,1.44)	(1.60,1.44)	(1.58,1.45)
CRD-3, Δ^C	63.59	62.05	69.56	72.62	70.09	63.22	63.24	63.31
CRD-4, Δ^C								
CRD-2, Δ^C	(1.37,1.70)	(1.59,1.68)	(1.49,1.72)	(1.04,1.72)	(1.49,1.73)	(1.53,1.68)	(1.53,1.68)	(1.51,1.68)
	63.14	61.48	70.06	71.81	70.75	62.86	62.87	62.93
CRD-5, Δ^C	(1.57,1.28)	(1.76,1.22)	**(1.67,1.30)**	**(1.16,1.33)**	**(1.67,1.31)**	(1.69,1.25)	(1.69,1.25)	(1.68,1.25)
	82.76	81.37	**91.87**	**94.01**	**92.08**	82.57	82.48	82.34
CRD-6, Δ^C	(1.45,1.62)	(1.70,1.55)	(1.57,1.64)	(1.14,1.64)	(1.56,1.65)	(1.61,1.57)	(1.61,1.57)	(1.59,1.58)
	63.72	62.21	69.74	73.45	69.97	63.44	63.47	63.42

low risk), three SC sizes for each one-dimensional chain ($N = 3, 5, 15$)(i.e., small to large numbers of SC partners), and three simulation periods ($T = 30, 180, 360$) (i.e., short to long periods), as illustrated in Tables 4–6. The sensitivity analysis for these parameters provides a wide range of possible instances, each of which was simulated 200 times.

The results (Tables 4–6) validate the robustness of the best speed for recovery from cyber-related disruptions (i.e., matching the SC firm's intangibles state with its immediate neighbors' highest intangibles state; CRD-5). However, for supply-related disruptions, the best recovery speeds differ slightly. This difference is attributed to interdependency between SC partners. As noted, a firm implementing the incremental speed (SRD-2) increases its operational state even if its neighbors remain in the "low" operational states. This incremental recovery speed from supply-related disruptions is more independent than the benchmarking speeds (SRD-3 and SRD-4), in which the firm's operational state is not be upgraded if its neighbors have low operational states. Moreover, the matching speed (SRD-5) is the least independent and the slowest recovery speed. Hence, when supply-related disruption risk is high, choosing an independent upgrade for the operational state is risky (Table 4); the firm could overconsume its resources but then fail to generate the equivalent SC performance (i.e., resource acquisition) if its neighbors still have low operational capabilities. In this case, the matching speed (SRD-5) is the most suitable because it avoids unnecessary resource consumption. However, when the supply-related disruption risk is low, concern about resource overconsumption is limited, and the firm should choose an option that enables it to aggressively improve its operational state. In this condition, the incremental speed (SRD-2) is the best, followed by the rigorous benchmarking (SRD-4).

Table 5 indicates that, when the SC size is sufficiently large ($N = 15$), SC firms should avoid the matching speed (SRD-5) when recovering from supply-related disruptions because firms in large SCs have difficulty perceiving other SC partners' (not immediate neighbors') changes to the operational states and are thus less sensitive to the interdependency among its SC partners. By contrast, the benchmarking speeds (SRD-4 and SRD-3) have the advantage of independently upgrading the firm's operational state from "low" to "medium"; thus, the effect of insensitivity to other SC partners' operational states under benchmarking speeds is not crucial. Moreover, when both benchmarking choices yield the same operational state for an SC firm, the rigorous benchmarking recovery speed is more reliable than the relaxed benchmarking recovery speed for ensuring equivalent resource acquisition; thus, SRD-4 has a slight edge over SRD-3 and is the best recovery speed when the SC size is sufficiently large. By contrast, when the chain size is small ($N = 3$), SC firms can easily perceive other SC partners' upgrades to the operational states; therefore, the matching (SRD-5) and relaxed benchmarking (SRD-3) speeds are favorable for recovering from supply-related disruptions.

Table 6 shows the results for short and long simulation periods. The matching choice for supply-related disruptions is not sensitive to short simulation periods because an SC firm is less likely to perceive whether and when its SC partners upgrade their operational states. Hence, the rigorous benchmarking (SRD-4), which is faster and more reliable, is the best speed for short simulation periods ($T = 30$). When simulated period is increased to $T = 360$, the SC firm has a higher likelihood of eventually perceiving its neighbors' operational state upgrades; thus, slower and less reliable recovery speeds, including the relaxed benchmarking (SRD-3) and matching (SRD-5) speeds, yield the best results.

We generalize the findings from the base case and the sensitivity analyses in Remark 1.

Remark 1. Three recovery speeds, namely rigorous benchmarking (SRD-4), relaxed benchmarking (SRD-3), and matching (SRD-5), are the only choices that cloud SC firms should consider when restoring their operational capabilities following supply-related disruptions. Moreover, the matching (CRD-5) is the best speed for restoring intangible capabilities following cyber-related disruptions; this choice is robust in the sensitivity analyses.

Table 4
Impact of supply-related disruption risk.

High supply-related disruption risk $\left(f_x = \frac{17}{365}, g_x = \frac{134}{365}\right)$								
	SRD-1	SRD-2	SRD-3	SRD-4	SRD-5	SRD-6	SRD-7	SRD-8
CRD-1, Δ^P CRD-3, Δ^P CRD-4, Δ^P	(1.13,1.12) 34.35	(1.31,0.86) 24.97	(1.13,1.22) 47.75	(0.68,0.97) 33.84	(1.10,1.36) 52.55	(1.33,0.95) 32.07	(1.33,0.95) 32.09	(1.33,0.97) 32.85
CRD-2, Δ^P	(1.04,1.51) 33.64	(1.30,1.18) 24.33	(1.08,1.45) 46.73	(0.68,1.26) 33.11	(1.04,1.60) 52.40	(1.28,1.28) 31.30	(1.28,1.28) 31.32	(1.28,1.30) 32.05
CRD-5, Δ^P	(1.18,0.95) 44.83	(1.37,0.76) 32.91	(1.19,1.00) 65.68	(0.69,0.89) 45.95	**(1.17,1.04)** **74.95**	(1.38,0.84) 42.01	(1.38,0.84) 41.98	(1.38,0.85) 43.03
CRD-6, Δ^P	(1.07,1.43) 34.08	(1.30,1.14) 24.79	(1.10,1.42) 47.35	(0.68,1.23) 33.54	(1.06,1.55) 52.49	(1.30,1.23) 31.79	(1.30,1.23) 31.00	(1.29,1.25) 32.54
CRD-1, Δ^C CRD-3, Δ^C CRD-4, Δ^C	(1.06,1.29) 34.08	(1.27,0.93) 24.57	(1.07,1.24) 47.14	(0.67,1.02) 33.86	(1.04,1.41) 53.18	(1.29,1.04) 31.55	(1.29,1.04) 31.57	(1.29,1.06) 32.36
CRD-2, Δ^C	(1.00,1.56) 33.35	(1.19,1.44) 24.12	(1.01,1.57) 46.54	(0.65,1.51) 33.32	(0.97,1.65) 53.53	(1.21,1.46) 30.93	(1.21,1.46) 30.94	(1.21,1.47) 31.71
CRD-5, Δ^C	(1.16,1.06) 44.49	(1.34,0.87) 32.27	(1.15,1.08) 64.77	(0.68,0.98) 45.78	**(1.13,1.13)** **75.81**	(1.36,0.0.94) 41.56	(1.36,0.94) 41.56	(1.35,0.0.95) 42.59
CRD-6, Δ^C	(1.07,1.43) 34.08	(1.30,1.14) 24.79	(1.10,1.42) 47.35	(0.68,1.23) 33.54	(1.06,1.55) 52.49	(1.30,1.23) 31.79	(1.30,1.23) 31.80	(1.29,1.25) 32.53
Low supply-related disruption risk $\left(f_x = \frac{7}{365}, g_x = \frac{10}{365}\right)$								
	SRD-1	SRD-2	SRD-3	SRD-4	SRD-5	SRD-6	SRD-7	SRD-8
CRD-1, Δ^P CRD-3, Δ^P CRD-4, Δ^P	(1.86,1.73) 127.62	(1.94,1.75) 132.41	(1.88,1.74) 127.78	(1.87,1.75) 130.23	(1.88,1.74) 127.87	(1.89,1.73) 127.87	(1.89,1.73) 127.90	(1.89,1.73) 127.73
CRD-2, Δ^P	(1.81,1.83) 129.66	(1.94,1.85) 135.20	(1.85,1.83) 129.86	(1.83,1.84) 132.60	(1.84,1.84) 129.92	(1.86,1.83) 130.00	(1.86,1.83) 129.99	(1.85,1.83) 129.77
CRD-5, Δ^P	(1.92,1.55) 157.48	**(1.96,1.57)** **163.20**	(1.93,1.55) 157.73	**(1.91,1.57)** **160.84**	(1.93,1.56) 157.79	(1.93,1.55) 157.86	(1.93,1.55) 157.98	(1.93,1.55) 157.88
CRD-6, Δ^P	(1.84,1.82) 120.01	(1.94,1.83) 132.97	(1.87,1.82) 128.20	(1.85,1.83) 130.75	(1.86,1.82) 128.27	(1.88,1.82) 128.28	(1.88,1,82) 128.31	(1.87,1.82) 128.11
CRD-1, Δ^C CRD-3, Δ^C CRD-4, Δ^C	(1.82,1.74) 127.03	(1.93,1.75) 132.13	(1.85,1.74) 127.33	(1.83,1.76) 129.86	(1.85,1.74) 127.33	(1.86,1.74) 127.40	(1.86,1.74) 127.40	(1.85,1.73) 127.06
CRD-2, Δ^C	(1.79,1.84) 129.18	(1.89,1.85) 134.51	(1.82,1.84) 129.60	(1.79,1.85) 132.33	(1.82,1.84) 129.63	(1.83,1.84) 129.63	(1.83,1.84) 129.63	(1.83,1.84) 129.24
CRD-5, Δ^C	(1.91,1.57) 157.34	**(1.96,1.58)** **162.88**	(1.92,1.56) 157.10	**(1.89,1.58)** **160.22**	(1.92,1.57) 156.92	(1.92,1.57) 157.27	(1.92,1.56) 157.34	(1.92,1.56) 157.08
CRD-6, Δ^C	(1.84,1.82) 127.97	(1.94,1.83) 132.95	(1.87,1.82) 128.25	(1.85,1.83) 130.72	(1.86,1.82) 128.24	(1.88,1.82) 128.32	(1.87,1.82) 128.34	(1.87,1.82) 128.01

4.2. Impact of cloud deployment on recovery speeds from supply-related disruptions

This subsection provides a discussion of the impact of cloud deployment on SC firms' recovery from supply-related disruptions. We investigate whether a firms' best recovery speed would change after adopting cloud services.

To facilitate this investigation, we assume that the SC firms with on-site data centers are subject to negligible cyber-related disruption; thus, in the CA simulation, we denote CRD-0 as the case in which firms do not need to have a speed of recovery from cyber-related disruptions. However, these firms also forfeit the benefits of cloud technology (i.e., the maximum level of intangible capabilities, which can further augment the SC performance). To represent the intangibles state of an SC firm with an on-site data center, we maintain this state at the "medium" level (i.e., $y'_{k,i}(t) = y_{k,i}(t) \equiv 1$). The SC firm's intangibles state could not be downgraded to "low" because cyber-related disruptions are unlikely, but it also could not be upgraded to "high" without the benefits of cloud services.

Table 7 lists the best recovery speeds for firms with and without cloud deployment under various scenarios. As mentioned, SC firms without the cloud have no recovery speed following cyber-related disruptions (i.e., CRD-0), whereas those with cloud deployment can adopt the matching (CRD-5) recovery speed for cyber-related disruptions. Thus, Table 7 provides a comparison of the best recovery speeds following supply-related disruptions. Choices in Table 7 with bold letters indicate that firms with and without cloud deployment should implement different recovery speeds following supply-related disruptions. For example, under low supply-related disruption risk, SRD-6 is a suitable choice for recovery for firms without cloud technology, but it is not an option for those with the cloud. For firms adopting cloud technology, the rigorous benchmarking (SRD-4) recovery speed is not considered for sufficiently long

Table 5
Impact of SC size.

$N = 3$	SRD-1	SRD-2	SRD-3	SRD-4	SRD-5	SRD-6	SRD-7	SRD-8
CRD-1,Δ^P CRD-3,Δ^P CRD-4,Δ^P	(1.52,1.45) 64.42	(1.72,1.39) 62.98	(1.61,1.50) 62.96	(0.99,1.45) 65.56	(1.61,1.51) 73.21	(1.65,1.41) 64.22	(1.65,1.41) 64.11	(1.64,1.41) 64.09
CRD-2,Δ^P	(1.42,1.67) 63.94	(1.69,1.59) 62.71	(1.53,1.69) 73.30	(0.97,1.64) 65.00	(1.52,1.71) 73.77	(1.59,1.62) 63.73	(1.59,1.62) 63.62	(1.57,1.62) 63.59
CRD-5,Δ^P	(1.60,1.22) 83.78	(1.78,1.16) 83.24	**(1.69,1,26) 96.91**	(1.02,1.27) 85.73	**(1.68,1.26) 97.10**	(1.72,1.19) 83.83	(1.72,1.19) 83.93	(1.71,1.19) 83.84
CRD-6,Δ^P	(1.46,1.62) 64.17	(1.70,1.56) 62.89	(1.56,1.66) 73.06	(0.98,1.61) 65.36	(1.55,1.67) 73.46	(1.62,1.58) 63.97	(1.62,1.58) 63.90	(1.60,1.58) 63.90
CRD-1, Δ^C CRD-3, Δ^C CRD-4,Δ^C	(1.45,1.52) 64.04	(1.69,1.42) 62.70	(1.56,1.54) 73.13	(0.96,1.47) 65.22	(1.56,1.56) 73.45	(1.61,1.45) 63.79	(1.61,1.45) 63.73	(1.59,1.46) 63.75
CRD-2, Δ^C	(1.38,1.70) 63.68	(1.59,1.69) 62.24	(1.48,1.73) 73.78	(0.92,1.72) 64.79	(1.48,1.74) 74.40	(1.54,1.69) 63.50	(1.54,1.69) 63.41	(1.52,1.69) 63.42
CRD-5, Δ^C	(1.58,1.28) 82.99	(1.76,1.23) 82.26	**(1.66,1.32) 96.66**	(0.99,1.32) 84.82	**(1.66,1.33) 96.87**	(1.70,1.26) 83.02	(1.70,1.26) 83.07	(1.69,1.26) 82.99
CRD-6, Δ^C	(1.46,1.63) 64.22	(1.70,1.56) 62.90	(1.56,1.66) 73.03	(0.98,1.61) 65.36	(1.55,1.67) 73.35	(1.62,1.58) 64.00	(1.62,1.58) 63.91	(1.60,1.58) 63.87

$N = 15$	SRD-1	SRD-2	SRD-3	SRD-4	SRD-5	SRD-6	SRD-7	SRD-8
CRD-1, Δ^P CRD-3, Δ^P CRD-4, Δ^P	(1.51,1.43) 63.61	(1.71,1.38) 61.71	(1.61,1.45) 65.94	(1.33,1.52) 79.53	(1.61,1.46) 66.14	(1.64,1.39) 63.41	(1.64,1.39) 63.35	(1.62,1.39) 63.31
CRD-2, Δ^P	(1.40,1.66) 62.97	(1.69,1.58) 61.35	(1.53,1.66) 65.64	(1.28,1.67) 78.82	(1.53,1.67) 65.90	(1.57,1.61) 62.73	(1.57,1.61) 62.69	(1.55,1.61) 62.65
CRD-5, Δ^P	(1.59,1.20) 83.10	(1.77,1.15) 81.92	(1.69,1.21) 86.50	**(1.41,1.30) 103.96**	(1.69,1.21) 86.82	(1.71,1.17) 83.20	(1.71,1.17) 83.10	(1.69,1.17) 82.89
CRD-6, Δ^P	(1.44,1.61) 63.38	(1.69,1.55) 61.60	(1.56,1.62) 65.86	(1.31,1.66) 79.36	(1.56,1.63) 66.06	(1.60,1.57) 63.14	(1.60,1.57) 63.09	(1.57,1.57) 63.04
CRD-1, Δ^C CRD-3, Δ^C CRD-4, Δ^C	(1.43,1.50) 63.20	(1.68,1.41) 61.46	(1.57,1.50) 65.76	(1.27,1.52) 78.55	(1.56,1.51) 65.92	(1.59,1.44) 62.87	(1.59,1.44) 62.81	(1.57,1.44) 62.95
CRD-2, Δ^C	(1.36,1.69) 62.74	(1.58,1.68) 60.85	(1.49,1.71) 66.01	(1.19,1.73) 78.17	(1.49,1.71) 66.15	(1.52,1.68) 62.43	(1.52,1.68) 62.37	(1.50,1.68) 62.53
CRD-5, Δ^C	(1.57,1.27) 82.28	(1.75,1.22) 80.73	(1.67,1.28) 85.87	**(1.35,1.34) 102.39**	(1.67,1.28) 86.29	(1.69,1.24) 82.23	(1.68,1.24) 82.24	(1.67,1.24) 82.08
CRD-6, Δ^C	(1.44,1.61) 63.39	(1.69,1.55) 61.70	(1.56,1.62) 65.86	(1.31,1.66) 79.17	(1.56,1.63) 66.01	(1.60,1.57) 63.10	(1.60,2.57) 63.04	(1.57,1.57) 63.17

simulation periods or for small chain sizes. In addition, firms with the cloud avoid the market-driven (SRD-6) recovery speed when the supply-related disruption risk is low. By contrast, SC firms with the cloud favor slower recovery speeds. As shown in the base case and in the case with long simulation periods, the relaxed benchmarking (SRD-3) and matching (SRD-5) recovery speeds are added to the list of the best recovery choices.

In summary, for each scenario presented in Table 7, SC firms with cloud technology tend to implement slower recovery speeds following supply-related disruptions, and those without the cloud tend to adopt faster speeds. This is not coincidental; in addition to consuming resources for recovery from supply-related disruptions, SC firms must consume resources to regain their intangible capabilities after cyber-related damages. Thus, when facing supply-related disruptions, SC firms with the cloud should implement more conservative and slower recovery speeds to avoid resource overconsumption.

We conclude these results in Remark 2.

Remark 2. Migration to cloud technology enables SC firms to adopt slower recovery speeds following supply-related disruptions.

5. Managerial implications

When SC firms are affected by disruption, they are conventionally suggested to quickly compensate for the disrupted SC flows and affected operational performance (e.g., lost sales, stockouts, production shutdowns, and delivery delays); this is referred to as the quick response in studies on production and manufacturing (Sodhi and Tang, 2009; Macdonald and Corsi, 2013; Ivanov et al., 2017). Quick responses have also been recommended for logistics after disruptions such as transportation accidents and disasters. For example, Sheu (2007) considered a three-layer emergency logistics co-distribution to quickly provide urgent relief following disasters. Loree and

Table 6
Impact of the simulation periods.

$T = 30$	SRD-1	SRD-2	SRD-3	SRD-4	SRD-5	SRD-6	SRD-7	SRD-8
CRD-1, Δ^P	(1.57,1.51)	(1.74,1.47)	(1.64,1.51)	(1.49,1.55)	(1.64,1.51)	(1.66,1.49)	(1.66,1.49)	(1.65,1.49)
CRD-3, Δ^P	15.65	15.17	15.97	17.68	15.97	15.32	15.31	15.33
CRD-4, Δ^P								
CRD-2, Δ^P	(1.52,1.69)	(1.73,1.64)	(1.59,1.69)	(1.45,1.71)	(1.59,1.69)	(1.62,1.67)	(1.62,1.67)	(1.60,1.67)
	15.02	14.70	15.40	17.10	15.39	14.74	14.73	14.76
CRD-5, Δ^P	(1.59,1.46)	(1.76,1.42)	(1.65,1.47)	**(1.50,1.50)**	(1.65,1.47)	(1.68,1.45)	(1.68,1.45)	(1.66,1.45)
	17.62	17.27	18.04	**20.16**	18.09	17.31	17.29	17.29
CRD-6, Δ^P	(1.54,1.63)	(1.73,1.59)	(1.62,1.63)	(1.47,1.66)	(1.61,1.63)	(1.64,1.61)	(1.64,1.61)	(1.63,1.61)
	15.27	14.87	15.61	17.33	15.61	14.97	14.97	14.98
CRD-1, Δ^C	(1.51,1.56)	(1.71,1.52)	(1.59,1.56)	(1.43,1.58)	(1.58,1.56)	(1.62,1.54)	(1.62,1.54)	(1.60,1.54)
CRD-3, Δ^C	15.56	14.98	15.92	17.62	15.89	15.17	15.15	15.16
CRD-4, Δ^C								
CRD-2, Δ^C	(1.46,1.73)	(1.64,1.72)	(1.54,1.73)	(1.38,1.75)	(1.54,1.53)	(1.57,1.72)	(1.57,1.72)	(1.56,1.72)
	15.00	14.52	15.46	17.15	15.42	14.70	14.67	14.67
CRD-5, Δ^C	(1.55,1.52)	(1.72,1.48)	(1.62,1.52)	**(1.45,1.54)**	(1.61,1.52)	(1.64,1.51)	(1.64,1.50)	(1.63,1.51)
	17.40	16.89	17.86	**19.95**	17.87	17.03	16.99	17.04
CRD-6, Δ^C	(1.54,1.63)	(1.73,1.59)	(1.62,1.63)	(1.47,1.66)	(1.61,1.63)	(1.64,1.61)	(1.64,1.61)	(1.63,1.61)
	15.29	14.83	15.64	17.35	15.60	14.99	14.95	14.96
$T = 360$	SRD-1	SRD-2	SRD-3	SRD-4	SRD-5	SRD-6	SRD-7	SRD-8
CRD-1, Δ^P	(1.52,1.44)	(1.71,1.39)	(1.62,1.50)	(1.04,1.46)	(1.61,1.51)	(1.65,1.40)	(1.65,1.40)	(1.63,1.41)
CRD-3, Δ^P	122.09	118.86	136.57	132.57	136.96	121.83	121.83	121.96
CRD-4, Δ^P								
CRD-2, Δ^P	(1.41,1.68)	(1.69,1.59)	(1.53,1.69)	(1.01,1.64)	(1.52,1.71)	(1.59,1.62)	(1.59,1.62)	(1.56,1.62)
	121.62	118.51	137.92	131.40	138.57	121.36	121.33	121.44
CRD-5, Δ^P	(1.63,1.10)	(1.80,1.06)	**(1.72,1.15)**	(1.09,1.18)	**(1.72,1.15)**	(1.74,1.08)	(1.74,1.07)	(1.73,1.08)
	164.94	162.49	**186.44**	177.64	**187.31**	164.65	165.05	164.94
CRD-6, Δ^P	(1.45,1.63)	(1.70,1.56)	(1.56,1.66)	(1.02,1.62)	(1.56,1.68)	(1.61,1.58)	(1.61,1.58)	(1.59,1.58)
	121.89	118.78	136.87	132.28	137.64	121.63	121.59	121.74
CRD-1, Δ^C	(1.45,1.52)	(1.69,1.42)	(1.57,1.54)	(1.00,1.47)	(1.57,1.56)	(1.61,1.45)	(1.61,1.45)	(1.59,1.45)
CRD-3, Δ^C	121.61	118.64	136.84	131.35	137.36	121.42	121.31	121.21
CRD-4, Δ^C								
CRD-2, Δ^C	(1.38,1.70)	(1.59,1.69)	(1.49,1.73)	(0.95,1.72)	(1.49,1.75)	(1.54,1.69)	(1.54,0.1.69)	(1.52,1.69)
	121.28	117.91	138.72	130.32	140.14	121.21	121.09	121.01
CRD-5, Δ^C	(1.61,1.17)	(1.79,1.13)	**(1.71,1.21)**	(1.06,1.23)	**(1.70,1.22)**	(1.73,1.15)	(1.73,1.14)	(1.71,1.14)
	163.45	160.80	**187.08**	175.57	**186.85**	164.12	163.35	163.75
CRD-6, Δ^C	(1.45,1.63)	(1.70,1.56)	(1.56,1.66)	(1.03,1.62)	(1.56,1.68)	(1.61,1.58)	(1.61,1.58)	(1.61,1.58)
	121.91	118.93	136.67	132.62	137.36	121.80	121.70	121.60

Table 7
Comparison of the best recovery speeds for SC firms with and without cloud deployment.

Scenarios	On-site data center	Cloud
Base case	(CRD-0, SRD-4)	(CRD-5, [SRD-4, **SRD-5, SRD-3**])
High supply-related disruption risk $\left(f_x = \frac{17}{365}, g_x = \frac{134}{365}\right)$	(CRD-0, SRD-5)	(CRD-5, SRD-5)
Low supply-related disruption risk $\left(f_x = \frac{7}{365}, g_x = \frac{10}{365}\right)$	(CRD-0, [SRD-2, SRD-4, **SRD-6**])	(CRD-5, [SRD-2, SRD-4])
$N = 3$	(CRD-0, [SRD-5, SRD-3, **SRD-4**])	(CRD-5, [SRD-5, SRD-3])
$N = 15$	(CRD-0, SRD-4)	(CRD-5, SRD-4)
$T = 30$	(CRD-0, SRD-4)	(CRD-5, SRD-4)
$T = 360$	(CRD-0, **SRD-4**)	(CRD-5, $\begin{bmatrix}\text{SRD-N3}\\ \text{SRD-N5}\end{bmatrix}$)

1. (X,Y) are the best recovery speeds in which X are the choices for cyber-related disruptions and Y are the choices for supply-related disruptions.
2. $\begin{bmatrix}\text{U}\\ \text{W}\end{bmatrix}$ represents that U and W both are speeds for recovery from supply-related disruptions.
3. [A, B, C] represents the order of the best recovery speeds with respect to SC performance.

Aros-Vera (2018) studied the facility location problem through multiple location distributions and by arranging inventory allocations for urgent logistics following disasters. Arıkan et al. (2017), Liang et al. (2018), and Choi et al. (2019) have investigated relief for disruptions to air logistics through the fast adjustment of crew scheduling, aircraft routing, and flight scheduling.

Although quick responses have been widely adopted, some research gaps require further study. First, if quick responses (i.e., fast recovery speeds) can be supported by sufficient resources, then their ability to yield excellent SC performance should be investigated. Second, Bode and Wagner (2015) and Bode and Macdonald (2017) have noted the importance of the following three aspects for recovery speed (i.e., slow or fast responses): the dependence between upstream and downstream participants, the frequency of SC disruptions, and the SC complexity. Because these factors differ between SCs, quick responses may not always be the best choice following a disruption. Notably, Parajuli et al. (2021) studied the congestion of facilities caused by flow reallocation from the disrupted facilities in a logistics system, and they revealed that a fast response speed is not always desirable. Given these concerns, the present study provides valuable information to SC managers regarding the conditions under which they should execute faster and slower responses following supply- and cyber-related disruptions. SC managers are expected to encounter black swan events with increasing regularity, thus impacting SC firms' operational capabilities (e.g., production capacity and labor supply) and intangible capabilities (e.g., reputation and public trust). Moreover, they are expected to be involved in increasingly large SCs.

Accordingly, based on the simulation results in this study, we provide guidance to operations and logistics managers regarding the appropriate speed for recovery from disruptions in cloud SC systems (Fig. 2).

Recommended speeds for recovery from supply-related disruptions in cloud SCs: The present results are not in agreement with the conventional wisdom and indicate that SC firms with the cloud should respond slowly when recovering from supply-related disruptions. Rather than quickly regaining their full operational capabilities following disruptions, we suggest that operations and logistics managers in SC firms with cloud deployment should adopt rigorous benchmarking, relaxed benchmarking, or matching. Instead of radically upgrading the firm's operational state, these three speeds are slow. Moreover, these three approaches consider the interdependency of the firm with its immediate SC partners; in other words, the restoration of operational capabilities in an SC firm depends on the operational capabilities of its immediate neighbors.

However, under some exceptions, managers are recommended specific recovery speeds. If managers anticipate high supply-related disruption risk (e.g., some analysts believe that the coronavirus pandemic will remain for some time and incur additional operational problems), then they should only consider the matching speed (the slowest speed) to regain operational capabilities. In addition, current SC structures are highly complex, particularly in industries with large SCs with participants located worldwide, such as in the automobile industry. Thus, SC managers of firms in large SCs should only apply rigorous benchmarking. According to this approach, the firm should consume sufficient resources to improve its operational capabilities even if its SC neighbors halt their business operations.

Recommended speeds for recovery from cyber-related disruptions in cloud SCs: For recovery from cyber-related damage to a firm's intangible assets, the firm should slowly regain its intangible capabilities (e.g., reputation, brand image, and public trust) by matching its capabilities with the highest capabilities of its immediate neighbors. Notably, this slow recovery speed is robust regardless of the risk of supply-related disruptions and the complexity of the SC.

Adjustments to speeds of recovery from supply-related disruptions following the adoption of cloud technology: After migrating to the cloud, operations and logistics managers in SCs are recommended to adopt slower speeds for recovery from supply-related disruptions. This is because, following cyber-related disruption, SC firms with cloud deployment require additional resources to recover from both operational and intangible damages. To avoid overconsumption, managers should be aware of the appropriateness of the recovery speeds for firms with the on-site data centers. Table 7 lists the recommended adjustments following the migration to cloud technology.

6. Concluding remarks and future research directions

Globalization has increased supply-related disruption risks, and advancements in digital and information technologies, such as cloud deployment, have not only promoted operational performance in SC firms but also introduced the risk of cyber-related disruptions. Together, these developments have altered the business environment for SC firms. Supply-related disruptions can be caused by operational issues due to labor strikes, natural disasters (e.g., the 2011 Tōhoku earthquake and tsunami in Japan), and epidemics (e.g., the 2020 COVID-19 pandemic, which caused factory closure worldwide); cyber-related disruptions can be caused by cyberattacks intended to disrupt businesses or steal information through the cloud service providers of SC networks. The present study investigated the best speeds for recovery from these two disruption types. We developed a CA simulation to evaluate a firm's SC performance based on its operational capabilities (e.g., production capacity and labor supply) and intangible capabilities (e.g., reputation, brand image, and public trust).

Our findings are summarized as follows. First, the CA simulation results revealed three best speeds for an SC firm's recovery following supply-related disruptions. The first approach is the matching speed; in this speed, an SC firm recovers by upgrading its damaged operational capabilities to match the highest operational capabilities of its immediate SC neighbors, assuming that the operational capabilities of these neighbors are higher than those of the firm. This is a slow speed to restore the firm's operational capabilities. The other two approaches are benchmarking speeds (i.e., relaxed benchmarking and rigorous benchmarking), whereby the firm upgrades its operational capabilities to the maximum level if the operational capabilities of its immediate SC neighbors are at the maximum level; if not, the firm upgrades its operational capabilities to the medium level. This benchmarking approach is slow, but it is faster than the matching approach. Second, when recovering from cyber-related disruptions that downgrade intangible capabilities, the best recovery approach is to slowly upgrade the firm's intangible capabilities by using the matching speed. This restores damaged intangible capabilities by upgrading them to match the highest intangible capabilities of the immediate SC neighbors but only if one of these neighbors has intangible capabilities at a higher level. Third, slower recovery speeds from supply-related disruptions are more suitable for SCs with cloud technology than for those without cloud technology.

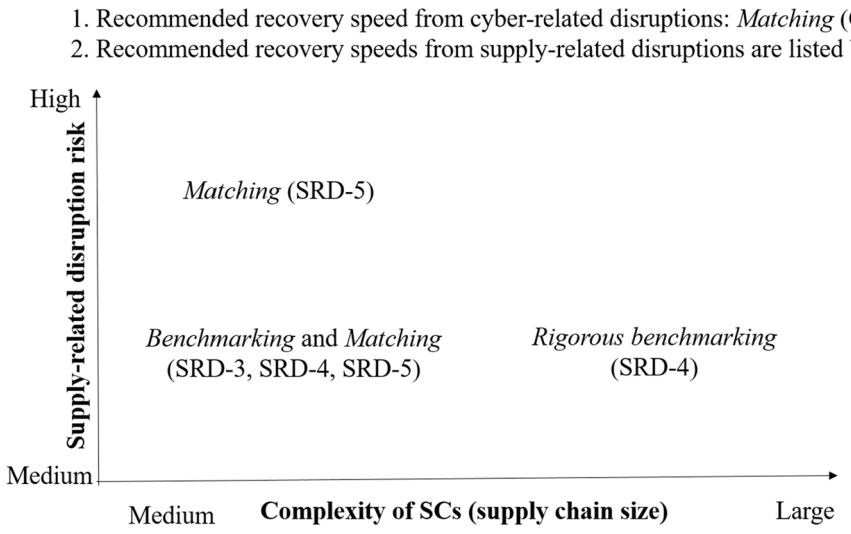

Fig. 2. Recommended recovery speeds by SC complexity and risk of supply-related disruption.

Several directions are suggested for future research as follows. First, the CA simulation in the present study included only the decisions related to an SC firm's recovery speed following disruptions, which incur resource consumption. Further studies could extend this by including resource consumption based on combining recovery speed with other recovery measures, such as establishing alternative suppliers, purchasing additional inventory, developing more capacity, and establishing backup suppliers (Ivanov et al., 2017); each of these measures would require different amounts of resources. Such twofold considerations could provide valuable insights for SC resilience. Second, the operational and intangibles states were based on subjective measurement; that is, we subjectively assigned three levels, which were also applied by Chen et al. (2015). In addition, the resources needed to upgrade a firm's two states were assumed to be identical. Future studies could use real-world data from various business and consumer databases to extend this research. Finally, some restrictions, such as the absence of interaction between a firm's operational capabilities and its intangible capabilities, could be relaxed. The settings in the present study assumed that cyber-related disruptions affect a firm's SC performance independently through the loss of intangible capabilities. However, in some cases, operational capabilities may also be lost.

In summary, this study introduced a unique CA method for simulating speeds for recovery from supply- and cyber-related disruptions in cloud SC firms. These results are expected to provide a valuable foundation for further investigation.

CRediT authorship contribution statement

Li-Ming Chen: Conceptualization, Methodology, Software, Investigation, Writing - original draft, Writing - review & editing, Supervision. **Wei-Lun Chang:** Validation, Investigation, Writing - original draft.

Acknowledgements

We thank the editor-in-chief, associate editor, and anonymous referees for their time and thoughtful suggestions that will help improve the paper.

References

Akinrolabu, O., Nurse, J.R., Martin, A., New, S., 2019. Cyber risk assessment in cloud provider environments: Current models and future needs. Computers Security 101600.
Arıkan, U., Gürel, S., Aktürk, M.S., 2017. Flight network-based approach for integrated airline recovery with cruise speed control. Transport. Sci. 51 (4), 1259–1287.
Bharadwaj, A.S., 2000. A resource-based perspective on information technology capability and firm performance: an empirical investigation. MIS Quart. 169–196.
Bier, T., Lange, A., Glock, C.H., 2020. Methods for mitigating disruptions in complex supply chain structures: A systematic literature review. Int. J. Prod. Res. 58 (6), 1835–1856.
Bode, C., Wagner, S.M., 2015. Structural drivers of upstream supply chain complexity and the frequency of supply chain disruptions. J. Oper. Manage. 36, 215–228.
Bode, C., Macdonald, J.R., 2017. Stages of supply chain disruption response: Direct, constraining, and mediating factors for impact mitigation. Decision Sci. 48 (5), 836–874.
Bond, D., 2018. Hackers target cloud services, Financial Times. Retrieved from https://www.ft.com/content/4f990a78-537a-11e8-84f4-43d65af59d43.
Bruque-Cámara, S., Moyano-Fuentes, J., Maqueira-Marín, J.M., 2016. Supply chain integration through community cloud: Effects on SC performances. J. Purchasing Supply Manage. 22 (2), 141–153.
Chambers, J., 2020. Coronavirus should inspire businesses to prepare their supply chains for the future. Retrieved from https://fortune.com/2020/04/12/coronavirus-supply-chain-disruption-risk/.
Chen, I.J., Paulraj, A., 2004. Towards a theory of supply chain management: the constructs and measurements. J. Oper. Manage. 22 (2), 119–150.
Chen, L.M., Liu, Y.E., Yang, S.J.S., 2015. Robust supply chain strategies for recovering from unanticipated disasters. Transport. Res. Part E: Logist. Transport. Rev. 77, 198–214.

Cheng, L., Craighead, C.W., Wang, Q., Li, J.J., 2020. When is the Supplier's Message "Loud and Clear"? Mixed Signals from Supplier-Induced Disruptions and the Response. Decision Sci. 51 (2), 216–254.
Choi, T.M., 2021. Risk analysis in logistics systems: A research agenda during and after the COVID-19 pandemic. Transport. Res. Part E: Logist. Transport. Rev. 102190.
Choi, T.M., Wen, X., Sun, X., Chung, S.H., 2019. The mean-variance approach for global supply chain risk analysis with air logistics in the blockchain technology era. Transport. Res. Part E: Logist. Transport. Rev. 127, 178–191.
Choi, T.Y., Wu, Z., 2009. Triads in supply networks: theorizing buyer–supplier–supplier relationships. J. Supply Chain Manage. 45 (1), 8–25.
Chopra, S., 2020. The coronavirus has upended supply chains. Here's how companies can prepare for the next disruptions. Retrieved from https://insight.kellogg.northwestern.edu/article/coronavirus-upended-supply-chains-how-companies-can-prepare-disruption.
Chowdhury, P., Paul, S.K., Kaisar, S., Moktadir, M.A., 2021. COVID-19 pandemic related supply chain studies: a systematic review. Transport. Res. Part E: Logist. Transport. Rev. 102271.
CNN, 2011, June 29. Tech supply chain to 'fully recover' from Japan disaster by Fall. https://money.cnn.com/2011/06/29/technology/japan_supply_chain/index.htm, accessed on May, 30, 2020.
Craighead, C.W., Blackhurst, J., Rungtusanatham, M.J., Handfield, R.B., 2007. The severity of supply chain disruptions: design characteristics and mitigation capabilities. Decision Sci. 38 (1), 131–156.
Deloitte, 2014. 2014 global survey on reputation risk. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/gx_grc_Reputation@Risk%20survey%20report.pdf.
Duong, L.N.K., Chong, J., 2020. Supply chain collaboration in the presence of disruptions: a literature review. Int. J. Prod. Res. 58 (11), 3488–3507.
Dutta, P., Choi, T.M., Somani, S., Butala, R., 2020. Blockchain technology in supply chain operations: Applications, challenges and research opportunities. Transport. Res. Part E: Logist. Transport. Rev. 142, 102067.
Ellis, S., Santagate, J., Brown, V., Venkataswamy, S. K., Veronesi, L., 2017. IDC FutureScape: Worldwide Supply Chain 2018 Predictions. Retrieved from https://www.idc.com/getdoc.jsp?containerId=US43146317.
Fahimnia, B., Pournader, M., Siemsen, E., Bendoly, E., Wang, C., 2019. Behavioral operations and supply chain management–a review and literature mapping. Decision Sci. 50 (6), 1127–1183.
Fiksel, J., Polyviou, M., Croxton, K.L., Pettit, T.J., 2015. From risk to resilience: Learning to deal with disruption. MIT Sloan Manage. Rev. 56 (2), 79–86.
Forbes, 2016, April 26. Toyota 'Quake-Proof' supply chain that never was. Retrieved from https://www.forbes.com/sites/jwebb/2016/04/26/toyotas-quake-proof-supply-chain-that-never-was/#6377150e2101.
Forbes Insights, 2014. The reputational impact of IT risk. Retrieved from https://images.forbes.com/forbesinsights/StudyPDFs/IBM_Reputational_IT_Risk_REPORT.pdf.
Gintis, H., 2000. Game theory evolving: A problem-centered introduction to modeling strategic behavior. Princeton University Press.
Godfrey, M., Zulkernine, M., 2014. Preventing cache-based side-channel attacks in a cloud environment. IEEE Trans. Cloud Comput. 2 (4), 395–408.
Goldbeck, N., Angeloudis, P., Ochieng, W., 2020. Optimal supply chain resilience with consideration of failure propagation and repair logistics. Transport. Res. Part E: Logist. Transport. Rev. 133, 101830.
Gwebu, K.L., Wang, J., Wang, L., 2018. The role of corporate reputation and crisis response strategies in data breach management. J. Manage. Inform. Syst. 35 (2), 683–714.
Haraguchi, M., Lall, U., 2015. Flood risks and impacts: A case study of Thailand's floods in 2011 and research questions for supply chain decision making. Int. J. Disaster Risk Reduct. 14, 256–272.
Haren, P., Simch-Levi, D., 2020. How coronavirus could impact the global supply chain by mid-March. Harvard Bus. Rev. 28.
Hishamuddin, H., Sarker, R.A., Essam, D., 2012. A disruption recovery model for a single stage production-inventory system. Eur. J. Oper. Res. 222 (3), 464–473.
Hishamuddin, H., Sarker, R.A., Essam, D., 2013. A recovery model for a two-echelon serial supply chain with consideration of transportation disruption. Comput. Ind. Eng. 64 (2), 552–561.
Hou, Y., Wang, X., Wu, Y.J., He, P., 2018. How does the trust affect the topology of supply chain network and its resilience? An agent-based approach. Transport. Res. Part E: Logist. Transport. Rev. 116, 229–241.
Hu, X., Gurnani, H., Wang, L., 2013. Managing risk of supply disruptions: Incentives for capacity restoration. Prod. Operat. Manage. 22 (1), 137–150.
Ireland, R.D., Webb, J.W., 2007. A multi-theoretic perspective on trust and power in strategic supply chains. J. Oper. Manage. 25 (2), 482–497.
Ismail, N., 2018. The financial impact of data breaches is just the beginning. Retrieved from https://www.information-age.com/data-breaches-financial-impact-123470254/.
Ivanov, D., 2019. Disruption tails and revival policies: A simulation analysis of supply chain design and production-ordering systems in the recovery and post-disruption periods. Comput. Ind. Eng. 127, 558–570.
Ivanov, D., 2020. Predicting the impacts of epidemic outbreaks on global supply chains: A simulation-based analysis on the coronavirus outbreak (COVID-19/SARS-CoV-2) case. Transport. Res. Part E: Logist. Transport. Rev. 136, 101922.
Ivanov, D., Pavlov, A., Dolgui, A., Pavlov, D., Sokolov, B., 2016. Disruption-Driven supply chain (re)-planning and performance impact assessment with consideration of pro-active and recovery policies. Transport. Res. Part E: Logist. Transport. Rev. 90, 7–24.
Ivanov, D., Dolgui, A., Sokolov, B., Ivanova, M., 2017. Literature review on disruption recovery in the supply chain. Int. J. Prod. Res. 55 (20), 6158–6174.
Ivanov, D., Dolgui, A., Sokolov, B., 2019. The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. Int. J. Prod. Res. 57 (3), 829–846.
Ivanov, D., Dolgui, A., 2020. A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0. Prod. Planning Control 1–14.
Jacques, A., 2016. Managing supply chains from the cloud. Retrieved from https://pharmaceuticalcommerce.com/supply-chain-logistics/managing-supply-chains-cloud/.
Jafarian, A., Asgari, N., Mohri, S.S., Fatemi-Sadr, E., Farahani, R.Z., 2019. The inventory-routing problem subject to vehicle failure. Transport. Res. Part E: Logist. Transport. Rev. 126, 254–294.
Jonkman, S.N., Bočkarjova, M., Kok, M., Bernardini, P., 2008. Integrated hydrodynamic and economic modelling of flood damage in the Netherlands. Ecol. Econ. 66 (1), 77–90.
Kamalahmadi, M., Parast, M.M., 2016. A review of the literature on the principles of enterprise and supply chain resilience: Major findings and directions for future research. Int. J. Prod. Econ. 171, 116–133.
Khalili, S.M., Jolai, F., Torabi, S.A., 2017. Integrated production–distribution planning in two-echelon systems: a resilience view. Int. J. Prod. Res. 55 (4), 1040–1064.
Kim, Y., Chen, Y.S., Linderman, K., 2015. Supply network disruption and resilience: A network structural perspective. J. Oper. Manage. 33, 43–59.
Levitin, G., Xing, L., Dai, Y., 2018. Co-residence based data vulnerability vs. security in cloud computing system with random server assignment. Eur. J. Oper. Res. 267 (2), 676–686.
Li, J., Chan, F.T., 2013. An agent-based model of supply chains with dynamic structures. Appl. Math. Model. 37 (7), 5403–5413.
Li, J., Zheng, Y., Dai, B., Yu, J., 2020. Implications of matching and pricing strategies for multiple-delivery-points service in a freight O2O platform. Transport. Res. Part E: Logist. Transport. Rev. 136, 101871.
Li, X., 2020. Reducing channel costs by investing in smart supply chain technologies. Transport. Res. Part E: Logist. Transport. Rev. 137, 101927.
Liang, Z., Xiao, F., Qian, X., Zhou, L., Jin, X., Lu, X., Karichery, S., 2018. A column generation-based heuristic for aircraft recovery problem with airport capacity constraints and maintenance flexibility. Transport. Res. Part B: Methodol. 113, 70–90.
Lindner, M., Galán, F., Chapman, C., Clayman, S., Henriksson, D., Elmroth, E., 2010, October. The cloud supply chain: A framework for information, monitoring, accounting and billing. In 2nd International ICST Conference on Cloud Computing (CloudComp 2010).
Liu, W., Shanthikumar, J.G., Lee, P.T.W., Li, X., Zhou, L., 2021. Special issue editorial: Smart supply chains and intelligent logistics services. Transport. Res. Part E: Logist. Transport. Rev. 147, 102256.

Loree, N., Aros-Vera, F., 2018. Points of distribution location and inventory management model for Post-Disaster Humanitarian Logistics. Transport. Res. Part E: Logist. Transport. Rev. 116, 1–24.
Macdonald, J.R., Corsi, T.M., 2013. Supply chain disruption management: Severe events, recovery, and performance. J. Business Logist. 34 (4), 270–288.
Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., Ghalsasi, A., 2011. Cloud computing—the business perspective. Decis. Support Syst. 51 (1), 176–189.
Maziliauskaite, K., 2015. The cloud-What's in it for supply chain managers?. Retrieved from https://www.allthingssupplychain.com/cloud-whats-supply-chain-managers/.
Melville, N., Kraemer, K., Gurbaxani, V., 2004. Information technology and organizational performance: An integrative model of IT business value. MIS Quarterly 28 (2), 283–322.
Miller, J.H., Page, S.E., 2009. Complex adaptive systems: An introduction to computational models of social life. Princeton University Press.
Montgomery, D.C., 1991. Experiments with a single factor: the analysis of variance. Design Analy. Exp. 75–77.
Mu, Q., Fu, Z., Lysgaard, J., Eglese, R., 2011. Disruption management of the vehicle routing problem with vehicle breakdown. J. Oper. Res. Soc. 62 (4), 742–749.
Nair, A., Narasimhan, R., Choi, T.Y., 2009. Supply networks as a complex adaptive system: Toward simulation-based theory building on evolutionary decision making. Decision Sci. 40 (4), 783–815.
Nair, A., Vidal, J.M., 2011. Supply network topology and robustness against disruptions–an investigation using multi-agent model. Int. J. Prod. Res. 49 (5), 1391–1404.
Namdar, J., Li, X., Sawhney, R., Pradhan, N., 2018. Supply chain resilience for single and multiple sourcing in the presence of disruption risks. Int. J. Prod. Res. 56 (6), 2339–2360.
Niu, B., Mu, Z., Cao, B., Gao, J., 2021. Should multinational firms implement blockchain to provide quality verification? Transport. Res. Part E: Logist. Transport. Rev. 145, 102121.
Parajuli, A., Kuzgunkaya, O., Vidyarthi, N., 2021. The impact of congestion on protection decisions in supply networks under disruptions. Transport. Res. Part E: Logist. Transport. Rev. 145, 102166.
Pathak, S.D., Day, J.M., Nair, A., Sawaya, W.J., Kristal, M.M., 2007. Complexity and adaptivity in supply networks: Building supply network theory using a complex adaptive systems perspective. Decision Sci. 38 (4), 547–580.
Paul, S.K., Sarker, R., Essam, D., 2014. Real time disruption management for a two-stage batch production–inventory system with reliability considerations. Eur. J. Oper. Res. 237 (1), 113–128.
Petrovic, D., Kalata, M., 2019. Multi-objective optimisation of risk and business strategy in real-world supply networks in the presence of uncertainty. J. Oper. Res. Soc. 70 (11), 1869–1884.
Ponomarov, S.Y., Holcomb, M.C., 2009. Understanding the concept of supply chain resilience. Int. J. Logist. Manage. 20 (1), 124–143.
Qi, G., Tsai, W.T., Li, W., Zhu, Z., Luo, Y., 2017. A cloud-based triage log analysis and recovery framework. Simul. Model. Pract. Theory 77, 292–316.
Rai, A., Patnayakuni, R., Seth, N., 2006. Firm performance impacts of digitally enabled supply chain integration capabilities. MIS Quart. 225–246.
Ritchie, B., Brindley, C., 2007. An emergent framework for supply chain risk management and performance measurement. J. Oper. Res. Soc. 58 (11), 1398–1411.
Ritter, T., 1999. The networking company: antecedents for coping with relationships and networks effectively. Ind. Mark. Manage. 28 (5), 467–479.
Robertson, D. A., Caldart, A. A., 2009. The dynamics of strategy: Mastering strategic landscapes of the firm. OUP Oxford.
Rose, A., 2004. Economic principles, issues, and research priorities in hazard loss estimation. In: Modeling spatial and economic impacts of disasters. Springer, Berlin, Heidelberg, pp. 13–36.
Roumani, Y., Nwankpa, J.K., 2019. An empirical study on predicting cloud incidents. Int. J. Inf. Manage. 47, 131–139.
Sahi, A., Lai, D., Li, Y., 2016. Security and privacy preserving approaches in the eHealth clouds with disaster recovery plan. Comput. Biol. Med. 78, 1–8.
Sawik, T., 2017. A portfolio approach to supply chain disruption management. Int. J. Prod. Res. 55 (7), 1970–1991.
Sheffi, Y., Rice Jr, J.B., 2005. A supply chain view of the resilient enterprise. MIT Sloan Manage. Rev. 47 (1), 41.
Sheffi, Y., 2005. The resilient enterprise: overcoming vulnerability for competitive advantage. MIT Press Books, p. 1.
Sheu, J.B., 2007. An emergency logistics distribution approach for quick response to urgent relief demand in disasters. Transport. Res. Part E: Logist. Transport. Rev. 43 (6), 687–709.
Siddiqui, A.W., Verma, M., 2015. A bi-objective approach to routing and scheduling maritime transportation of crude oil. Transport. Res. Part D: Transport Environ. 37, 65–78.
Sodhi, M.S., Lee, S., 2007. An analysis of sources of risk in the consumer electronics industry. J. Oper. Res. Soc. 58 (11), 1430–1439.
Sodhi, M.S., Tang, C.S., 2009. Managing supply chain disruptions via time-based risk management. In: Managing supply chain risk and vulnerability. Springer, London, pp. 29–40.
Tan, W.J., Cai, W., Zhang, A.N., 2020. Structural-aware simulation analysis of supply chain resilience. Int. J. Prod. Res. 58 (17), 5175–5195.
Toka, A., Aivazidou, E., Antoniou, A., Arvanitopoulos-Darginis, K., 2013. Cloud computing in supply chain management: an overview. In *E-logistics and e-supply chain management: applications for evolving business*. IGI Global, pp. 218–231.
Torabi, S.A., Baghersad, M., Mansouri, S.A., 2015. Resilient supplier selection and order allocation under operational and disruption risks. Transport. Res. Part E: Logist. Transport. Rev. 79, 22–48.
Van Nguyen, T., Zhang, J., Zhou, L., Meng, M., He, Y., 2020. A data-driven optimization of large-scale dry port location using the hybrid approach of data mining and complex network theory. Transport. Res. Part E: Logist. Transport. Rev. 134, 101816.
Veneti, A., Makrygiorgos, A., Konstantopoulos, C., Pantziou, G., Vetsikas, I.A., 2017. Minimizing the fuel consumption and the risk in maritime transportation: A bi-objective weather routing approach. Comput. Oper. Res. 88, 220–236.
Wang, H., Tan, J., Guo, S., Wang, S., 2018. High-value transportation disruption risk management: Shipment insurance with declared value. Transport. Res. Part E: Logist. Transport. Rev. 109, 293–310.
Wang, J., Lim, M.K., Zhan, Y., Wang, X., 2020. An intelligent logistics service system for enhancing dispatching operations in an IoT environment. Transport. Res. Part E: Logist. Transport. Rev. 135, 101886.
Wilson, M.C., 2007. The impact of transportation disruptions on supply chain performance. Transport. Res. Part E: Logist. Transport. Rev. 43 (4), 295–320.
Wu, X., Zhang, R., Zeng, B., Zhou, S., 2013. A trust evaluation model for cloud computing. Procedia Comput. Sci. 17, 1170–1177.
Wu, Z., Choi, T.Y., 2005. Supplier–supplier relationships in the buyer–supplier triad: Building theories from eight case studies. J. Oper. Manage. 24 (1), 27–52.
Xu, S., Zhang, X., Feng, L., Yang, W., 2020. Disruption risks in supply chain management: a literature review based on bibliometric analysis. Int. J. Prod. Res. 58 (11), 3508–3526.
Yu, W., Chavez, R., Jacobs, M.A., Feng, M., 2018. Data-driven supply chain capabilities and performance: A resource-based view. Transport. Res. Part E: Logist. Transport. Rev. 114, 371–385.
Zhao, K., Zuo, Z., Blackhurst, J.V., 2019. Modelling supply chain adaptation for disruptions: An empirically grounded complex adaptive systems approach. J. Oper. Manage. 65 (2), 190–212.