Uncertain Supply Chain Management 11 (2023) 145–152

Contents lists available at GrowingScience

Uncertain Supply Chain Management

homepage: www.GrowingScience.com/uscm

The effect of information security on e-supply chain in the UAE logistics and distribution industry

Muhammad Turki Alshurideh[a,b*], Enass Khalil Alquqa[c], Haitham M. Alzoubi[d], Barween Al Kurdi[e] and Samer Hamadneh[f]

[a]*Department of Marketing, School of Business, The University of Jordan, Amman 11942, Jordan*
[b]*Department of Management, College of Business, University of Sharjah, Sharjah 27272, United Arab Emirates*
[c]*College of Art, Social Sciences and Humanities, University of Fujairah, United Arab Emirates*
[d]*School of Business, Skyline University College, Sharjah, United Arab Emirates*
[e]*Department of Marketing, Faculty of Economics and Administrative Sciences, The Hashemite University, Zarqa, P.O Box 330127, Zarqa 13133. Jordan*
[f]*Department of Marketing, School of Business, The University of Jordan, Amman 11942, Jordan*

A B S T R A C T

The effect of information security on the e-supply chain attracted attention to investigate its relationship with the mediating role of supply chain risk in the logistics and distribution industry in the United Arab Emirates (UAE). The proposed research explored the mediating effect of supply chain risk in the logistics and distribution industry, providing unique insights for future research, literature, and targeted sectors. A descriptive, causal and analytical design with quantitative research technique was applied to the proposed research model. A sample of 301 respondents from the managerial departments of 176 logistics and distribution companies in Dubai and Abu Dhabi was used to assess the research variables. The findings revealed that the impact of information systems was positively associated with the e-supply chain, while the indirect impact of supply chain risk significantly positively impacted the e-supply chain. The research is limited to assessing the supply chain risk as an intermediary. For future research, exploring the SC risk prevention strategies' impact on the E-supply chain is recommended. Research findings are anticipated to assist communities of practice in making better information security decisions in the context of e-supply chain by clearly implementing information security policies internally and externally to enhance e-supply chain performance and SC risk management.

Article history:
Received August 5, 2022
Received in revised format August 26, 2022
Accepted October 26 2022
Available online November 3 2022

Keywords:
Supply Chain Risk
Information Security
E-Supply Chain
Distribution Industry in the UAE

1. Introduction

Implementing information system technologies in organisations seems to manage functions worldwide in the technological era. It helps in improving the information within the firms and between the partners of the supply chain processes (Gölgeci, & Ponomarov, 2015). This secure sharing helps in the demand for information in the supply chain that can enhance the performance of the supply chain processes and overcome the issues that can increase the availability and reduce the inventory management-related costs (Attaran, 2007; Kurdi et al., 2022). Additionally, certain risks may arise for the entire industry (Hamadneh et al., 2021). Such risks could occur due to new technologies disrupting the whole market or a new competitor with a similar business model within the same industry (Kumar et al., 2019; Lee, Azmi, et al., 2022a; Shamout et al., 2022). The procedure of moving products around the globe is a lengthy and difficult process. Managers are still unaware of the necessary steps to improve their logistics security programmes in light of new difficulties in managing the efficiency of the e-supply chain (Alshurideh et al., 2022; Joghee et al., 2021). Without compromising supply chain effectiveness, the security concerns of manufacturers and transportation businesses must be addressed. Information security in the e-supply chain is necessary at each process segment (Lee, Romzi, et al., 2022b; Rafati, 2022). The logistics and distribution industry must consider the criteria to enhance technology adoption practices (Falasca et al., 2008; Sindhuja, 2014). In the era of technology and home delivery, companies have become more aware of safe delivery.

* Corresponding author
E-mail address m.alshurideh@ju.edu.jo (M. T. Alshurideh)

doi: 10.5267/j.uscm.2022.11.001

This research provides a model of supply chain risk that captures both the source of assaults and the e-supply chain activities and links susceptible to information technology threats in the logistics and distribution industry of the UAE. Even though suppliers in several tiers and different countries are fully coordinated to reduce the overall supply chain cost, significant risks and problems in global business operations could disrupt the global supply chain. Therefore, this research will incorporate the important factors that can help observe the risk and the organization's attempt to prevent these risks to competitiveness.

2. Theoretical framework

2.1 Information Security

Information security can be defined in terms of technical, formal, and informal levels. A technical level: First, let us discuss how well we can do this. Information security controls in computer systems include speech analysis, firewalls, digital signatures, and other methods to protect software, devices, and data within the computer system (Salloum et al., 2020). All of these methods are used to protect the applications of software, devices, and data that are within the computer system itself. Second, at the formal level, official controls are established based on rules that state how the published technical controls should be structured. At the informal level, the issue is how to keep information secure within an organization's structure (Kunnathur & Vaithianathan, 2008). A successful enterprise must protect its valuable information assets, such as its IT systems and networks (Cheung et al., 2021). Regarding e-commerce, many people assume that information technology security is a relatively new concept that has only been developed during this period.

2.2 E-Supply Chain

Supply chain specialists refer to electronic business processes in the supply chain as "e-Supply Chain" by supply chain specialists. This term entails any activity using electronic business operations across the supply chain. In the context of supply chain, E-supply chain management refers to using e-business technology to help and improve value-adding processes (Kumar et al., 2019). The use of technology to enhance business-to-business operations and make them quicker, more flexible and simpler to regulate is another definition of e-supply chain management described by (Chu et al., 2020). He continues: It also has the additional benefit of increasing client happiness. The development of supply chain management (e-SCM) entails more than simply technological developments. Supply chain management is concerned with changes in management policies, performance metrics, business processes, and organizational structures at all levels of the supply chain (Angerhofer & Angelides, 2006).

2.3 Supply Chain Risk

When new market trends like just-in-time (JIT) and significant non-core activities like supplier rationalization programs are implemented, the supply chain may become more vulnerable due to dispersion, centralization and globalization of the supply chain's components. Due to the risk of influencing performance, we should control it (Kumar et al., 2019). Furthermore, the risk may include a scenario in which an extremely unusual event occurs, with adverse consequences for the company. Supply chain risk may be defined in terms of the rate at which a potential outcome has an effect and its vulnerability to the impact. Specifically, risk refers to the unpredictability of an occurrence that has the potential to interrupt a single link in the E-supply chain and, as a consequence, influence the company's ability to achieve its objectives (Heckmann et al., 2015). This kind of risk is sometimes referred to as "e-supply chain volatility," which entails the potential of reducing value added at any point along the supply chain's journey due to changes in the amount or quality of commodities at any given point in time or location (Kumar et al., 2019). To minimize internal and external losses, a company's supply chain risk management strategy must be carefully and properly crafted and maintained. Some academics argue that resources for supply chain risk management should be increased. Others conducted a study involving various organizations and discovered that insufficient contingency planning was one of the primary reasons for supply chain interruptions (Gurtu & Johny, 2021).

2.4 Operational Definitions

Variables	Definition	Reference
Information Security	Information security safeguards sensitive data against unauthorized access, modification, recording, disruption, or destruction. The goal is to ensure the security and privacy of critical data, including financial information, customer account information, and intellectual property.	(Cheung et al., 2021)
Supply Chain Risk	SC risk refers to a collection of approaches, tactics, and strategies for mitigating the supply chain's susceptibility. Improved supply chain risk management (SCRM) practices may contribute to the development of resilience.	(Can Saglam et al., 2020)
E-Supply Chain	Business operations that integrate e-business strategies with supply chain processes are referred to as e-Supply Chain. Chain management for e-supplies includes utilizing e-business technologies to facilitate and maximise value-adding supply chain operations.	(Aloqool et al., 2022)

2.5 Industry Description

The UAE is an attractive market for retailers due to government-led economic reforms, a wide and digitally connected millennial customer sector with extensive spending power. The contribution of wholesale and retail trade to Dubai's GDP is

26.4 per cent, and the GDP of the UAE as a whole is approximately 11 per cent. Many companies aim to make the UAE one of the key markets for their products to take advantage of this dynamic market. Selecting a distributor for your items is one of the trading firms' most efficient operational structures. A distributor is in charge of the channel mix, product availability, and visibility, promoting purchasing your goods through various channels in the area. Distributors are typically regarded as the product's proprietors for the designated region. This industry is involved with extensive information of implementing information security and the criteria for e-supply chain by considering supply chain risk overall.

3. Literature review

3.1 The relationship and impact of information security on supply chain risk

The impact of information security on the e-supply chain defines the evolution of supply-chain processes over the last few years that are largely driven by technology. The companies move towards digital management that can compel the disruptions within previous years' services. Therefore, businesses are allowed to build the options of cyber security fortresses for their success in the market. Different vulnerabilities are used to define the touch points that can help the manufacturers, supplier services, global management of partners, and different service providers. The potential threats arise within the parties waiting to breach security for getting the initial chance. Cyber security is considered a mature action to a definite extent that can manage larger enterprises and focuses on implementing the perimeter within the organisation. There is a lack of governance and control over the management of individual departments dealing with identifying the related entities within the ecosystem (Hunitie et al., 2022; Qi et al., 2022). Several smaller businesses are considering the lower match for the implementation of the strengths of cyber security. The processes provide favourable impacts to the entry points for the definite hackers. Different supply chain information security (SCIS) issues are neither discussed in detail nor received the appropriate attention. The companies use a framework for bringing out certain issues for the enfolding of SCIS (Bolhari, 2009). There is a definite adoption by businesses as considering the complex management of the operations that can impact the processes efficiently. The experts point out that organisations are considering the least evaluation management and describing the potential possibilities of using blockchain analysis. Therefore, the organisations are responsible for implementing the corporate-wide vision for the data-access guidelines and related standards. It defines the sensitive data that can be shared within the services to manage the potential server and network audits. It will help maintain a good trail for special and admin services. The experts in the e-supply chain seem to promote the idea of defining the breach for the occurrence of a cyber-resilience plan as essential (Bolhari, 2009). There must be a broader framework that can support different sizes of businesses while measuring the e-supply-chain cyber security management. Based on previous literature, a hypothesised model can be supported in this research.

H_1: *Information system has a significant impact on supply chain risk.*

3.2 The relationship and impact of information security on the e-supply chain

Information Technology has become a vital component in supply chain collaborations due to its ability to process the huge amount of data and information needed to manage the processes, leading to a maximized efficiency for all participating members within the supply chain commands (Demeter & Gelei, 2004). Defining supply chain risk is critical to measuring and defining information security's effect. Supply chain risk is described as the potential for a failure to satisfy consumer needs if an incident or accident affects the movement of products from suppliers to markets. Manufacturing processes, control, demand, supply, and the environment are the key contributors to supply chain risk. The organization, network, and environment contribute to data collection (Pournader et al., 2020).

First, the organization’s risks can include issues with labor, production disruptions, IT systems, processes, warehousing, transportation, planning and scheduling. Additionally, network risks include unexpected situations in the employment and transportation of goods and services. Lastly, environmental risks are defined by accidents and socio-political actions impacting the supply and demand risks in the organization and network levels. In March and April of 2021, an employee's negligence caused massive data loss to the city of Dallas Police Department. The employee erased 8.7 million main police files collected as evidence for cases where the family violence unit owned most files. The prevention of such threats is the responsibility of the managers who can provide awareness to employees due to the important role played by information security awareness and knowledge. Moreover, plans, procedures and policies set in the right manner are proven to be vital in minimizing threats caused by employees within the organization (Bolhari, 2009). Virus, Browser Hijackers, Worm, Trojans, and Keyloggers are examples of external threats. To elaborate more, Keyloggers are programs that record users' keystrokes, including personal information and passwords. Browser Hijackers are programs that gather information on users' online habits every time they begin browsing. Literature suggests a significant relationship between information systems (IT) and the E-supply chain. The evidenced information is considered for this research's proposed hypothesis.

H_2: *Information system has a significant impact on the E-supply chain.*

3.3 The relationship and impact of supply chain risk on the e-supply chain

Due to globalization, international business, short product life cycles, and variation in consumer demand and requirements, risks in supply chain activities have risen in recent years. Such disruptions cause sudden and unanticipated failures that natural disasters may also cause, fire loss, lack of supplier power, war, terrorism and so on, "*involuntary loss of specific assets due to events caused by factors that are outside the government's control and is mostly political*" (Rajesh & Ravi, 2015). These risks are divided into categories which are divided into subcategories. This includes the risk of delays, incorrect forecasting, faulty systems, procurement and purchasing teams, and minimal inventory and capacity. The two main categories of risk faced by e-supply chains are divided into two factors: internal and external. The internal risk factors include internal faults such as delays in information flow throughout the supply chain or slow communication between the parties (Chu et al., 2020). For instance, the parties involved within the supply chain are exposed to inaccurate information due to misunderstandings. This can cause a risk. Moreover, customs regulations are considered as an internal risk and capacity variation. On the other hand, external factors include the threat of competition and market competitors, the prices within the market, "competitive pricing", and how competitors usually price their products. Furthermore, supplier quality is another risk factor that affects the e-supply chain (Baabdullah et al., 2019; Kumar et al., 2020). As discussed in Porter's five competitive forces, supplier quality can be a major issue whether you have the best quality product/service within the market or not. Besides the list, manufacturing costs and political/economical/technological and legal issues are considered risk factors affecting the e-supply chain industry. Risks often occur due to the inconsistent balance between supply and demand and random interruptions to the normal activities within the e-supply chain. The risks of the supply chain impacting the e-supply chain are reflected in the diagram below. Fig. 1 shows the relationship of the impact of both variables (Kumar et al., 2019; Pournader et al., 2020).

Fig. 1. E-Supply Chain Risk Model

The above risks are the related risk factors in the supply chain on the e-supply chain. The information & policy risk is related to secure information, copyrights, Intellectual property rights (IPR) and strategic information (Kumar et al., 2019). As for the environmental risk, the Macroeconomic risks are the external environment, usually referred to as "PESTEL", adding to it the natural disasters that may occur, such as extreme weather conditions (tornados, earthquakes, etc.). Regarding the relations risks, risks like lack of transparency, the ability to commit to these relationships and maintaining supplier relationships strong and solid (Alshurideh, 2022). Infrastructure risk involves all technological and economical risks, channels used for goods transportation, and whether the country's infrastructure is dependable enough for the success of the supply and e-supply chain (Pettit et al., 2019; M. Alshurideh et al., 2022; Kurdi et al., 2022). This leads to demand risks involving major changes in trends and buying patterns, fluctuations in demand and inaccurate forecasts in demand (Lee et al., 2022a,b; Yang et al., 2021). Sudden moves from competitors and unexpected cancellations in orders and short product lifecycles. Finally, this brings us to the organizational risks involving cultural risks, untrained staff, leadership issues, the organization's reputation, inbound and outbound logistics/operations and availability. The risk categories can be listed differently, starting with a variation. Based on previous literature, supply chain risks can affect the e-supply chain, which may put significance to the hypothesized model of this research.

H$_3$: *Supply chain risks have a significant impact on the e-supply chain.*

3.4 The relationship and impact of information security on supply chain risk with mediating effect of e-supply chain

New supply chain strategies are necessary to better prepare for market volatility and environmental disturbances' growing quantity and diversity. This is why delivery and shipping companies are more aware of the importance of having information security to protect their e-supply chain from various risks. As a result, supply chains must be adaptive to keep pace with the rapid pace of change. Securing the information during its flow in the e-supply chain is necessary and ensures having the right and updated information (Baabdullah et al., 2019). This is important because we may have some risks in the supply chain due to internal or external factors, as mentioned earlier. If not controlled, it would be challenging to sustain in the competitive environment and impact the final quick delivery in the e-supply chain, especially for unexpected disruptions. Electronic Data Integration is one way of securing the sharing of huge amounts of information with minimum risk and ambiguity (Tarafdar & Qrunfleh, 2017). Business risk has changed due to the more widespread use of information technology and the reliance on it for safe and continuous operations (Falasca et al., 2008; Stoneburner et al., 2002). To reduce supply chain risk, the new e-supply chain places a strong emphasis on information exchange and building connections with partners in a secure way. The strategic value of information technology (IT) reduces as it appears more in individual firms and supply networks. Thus, securing these systems while not incurring exorbitant expenditures is now the most challenging task. There is no question that the supply chain is adversely affected by information security hazards. This risk requires more investigation. Based on our findings, to enhance decision-making and SCM, we need to know more about the link between information security in the e-supply chain and its risk, especially for delivery and shipping companies (Chu et al., 2020; Kumar et al., 2019; Purwanto

et al., 2022). Despite the importance of supply chain security, there are few defined terms in the literature. In order to keep supply chain assets (such as commodities, buildings, equipment, or data) safe from theft, damage, or unauthorized access, policies, procedures, and technology are in place (weapons of mass destruction). This applies to the e-supply chain because there is more emphasis on the concept of information security and supply chain risk.

H4: *Information security significantly impacts the E-supply Chain with the mediating effect of Supply chain risk.*

3.5 Problem Statement & Research Gap

Although the benefits of Information security in the E-supply chain have been highlighted and agreed upon by several authors (Aloqool et al., 2022; Chu et al., 2020), some factors are rarely considered, such as the supply chain risk or its mediating role in information system and e-supply chain in distribution industry UAE. The current research thereby aims to fill the gap in the corpus of information in this area. Information security is determined to play a significant part in achieving secured supply chain management, which would enable organizations to improve their organizational performance, more investigation has to be done before making a final judgment on the risk's repercussions, which is a critical part of the decision-making process between information security and the e-supply chain. Supply chain management must study this area to ensure that the risk of information technology security is adequately addressed when businesses use technology to foster collaborative partnerships.

3.6 General Research Model

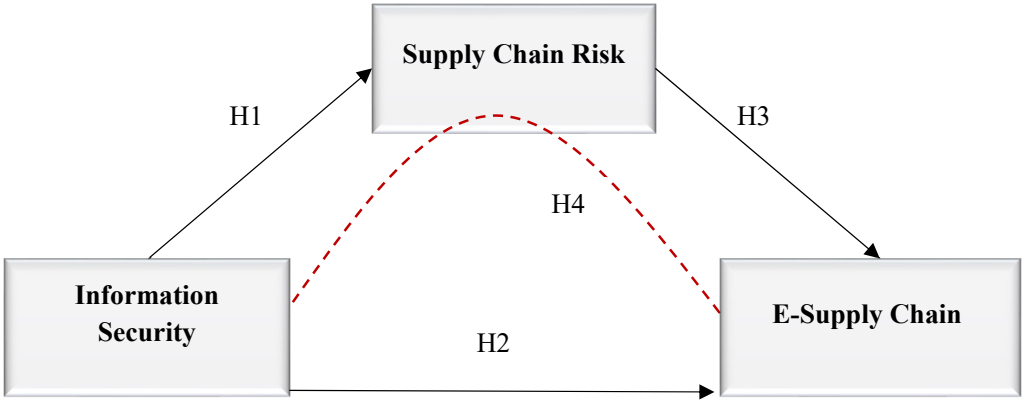

Fig. 1. Research Model

3.7 Research Hypothesis

HO1: Information Security has no statistical impact on Supply Chain Risk in the UAE Distribution Industry.
HO2: Information Security has no statistical impact on the e-Supply Chain in the UAE Distribution Industry.
HO3: Supply Chain Risk has no statistical impact on the e-Supply Chain in the UAE Distribution Industry.
HO4: Information Security has no statistical impact on the e-Supply Chain with the mediating effect of Supply Chain Risk at the UAE Distribution Industry.

3.8 Research Methodology and Design

To measure the relationship of research variables (Information Security, E-Supply Chain, and SC Risk), the required research design incorporated the distribution companies based in Dubai & Abu Dhabi, UAE. A convenient sampling technique was used to access the distribution center's managerial departments. A quantitative technique with the descriptive, exploratory, analytical, and causal design was applied. An online survey questionnaire was developed to gather the data via email medium. The questionnaire data was assessed with regression and hypothesis testing using ANOVA and SPSS.

3.9 Population, Sample & Unit of Analysis

The population for the proposed research targeted 179 Logistics & distribution companies located in Dubai & Abu Dhabi, UAE. A total of 600 questionnaires were sent via email, and a sample of 301 was received with valid results after screening. The correspondents of the survey were (Production manager, SC Manager, IT Manager & Product Distributor). To assess the variables, a 30-item questionnaire has been developed on a 5-point Likert scale (from 1, strongly disagree to 5, strongly agree). 11 items were used to assess the "Information Security" 9 items were used to assess "E-supply chain" and 10-items used to assess for "SC Risk".

4. Data analysis

4.1 Demographic Analysis

Based on the demographic data, male participants were 217 (72.1%) and female participants 84 (27.9%). This indicates that males have the largest number of IT managers from various distribution companies.

Gender Job Status

Fig. 2. Personal characteristics of the participants

4.2 Reliability, Descriptive & Correlation

The assessment of research variables was tested for validity and reliability before going for further analysis. The results of Cronbach's Alpha show the good reliability of each construct EI=.77, CP=.85, and OBB=.77, respectively. Moreover, the descriptive stats show that the mean value for Information security (M=3.45, SD=.77), the mean value for Supply Chain Risk with the lowest ranking (M=3.11, SD=.57). In contrast, E-Supply Chain indicates the highest ranking with the mean value (M=3.51, SD=.58). Table 1 also represents the correlation coefficient data summary that depicts a significant positive relationship of Information Security with Supply Chain Risk r=.826. P<0.05, Information Security has a significantly high correlation with E-supply chain as r=.752, and Supply chain risk is highly correlated with E-supply chain with r=.85, P<0.05. Table 1 shows the overall data summary.

Table 1
The correlation coefficient data summary that depicts a significant positive relationship of Information Security with Supply Chain Risk

Construct	No of items	Cronbach's α	Mean	S.D	Information Security	Supply Chain Risk	E-Supply Chain
Information Security	6	.777	3.45	.77	1		
Supply Chain Risk	7	.853	3.11	.57	.826**	1	
E-Supply Chain	6	.772	3.51	.58	.752**	.858**	1

IS=Information Security (M=3.45, SD=77%, SCR=Supply chain risk M=3.11, SD=57%, E-supply chain M=3.51, SD=58%.
*-Level of significance at P<0.05***

4.3 Multiple Regression & Hypothesis Testing

Table 2 presents the summary of the regression test to examine the hypotheses of the survey.

Table 2
Regression Analysis with mediating effect of Supply Chain Risk with ANOVA

Hypothesis	Regression Weights	Standardized Coefficients					
		β	*Adjusted R²*	*R²*	*Sig*	*t-value*	*Hypothesis*
H_1	IS→SCR	.752	.564	.566	.000	19.74	Yes
H_2	IS→E-SC	.826	.683	.682	.000	8.49	Yes
H_3	SCR→E-SC	.858	.735	.736	.000	14.24	Yes
H_4	Mediating effect of SC Risk IS*SCR→E-SC	.901	.810	.811	.000	10.92	Yes

**Level of Significance (α≤0.05)*
***Critical t-value (df/p) = 1.64*

5. Discussion of the results

This research demonstrates the significance of supply chain risks to achieving a successful e-supply chain. Table 2 illustrates that H1 has a significant relationship between information security and supply chain risk at (β=.752, t=19.74) and the variance as R^2=56%. The H1 is supported. On the other hand, the findings reveal a significant impact of supply chain risk on the E-supply chain with (β=.826, t=8.49) and predict a high variance between the information security and e-supply chain R^2=68%, supporting H2. The impact of supply chain risk has a significant impact on the e-supply chain, demonstrated by the data analysis and also evidenced in the literature (β=.858, t=14.24) and the variance shown in the variables. The increase in supply

chain risks affects the e-supply chain at R=73%. A high variance indicates a high dependency of the construct on each other. The H3 is also supported in this research. Further analysis depicts that the mediating effect has a significant relationship between information security and the e-supply chain. The data findings show (β=.901, t=10.92) a significant positive impact of supply chain risk as a mediator, and the variance among variables is R=81%. A high variance range is predicted as a high dependency on supply chain risk. The present framework provides gap-filling results that demonstrate that IT development and information security implementation in the supply chain process can prevent supply chain risks and adverse effects to the organization (Aloqool et al., 2022; Cheung et al., 2021; Kumar et al., 2019). The trend of the e-supply chain requires security attempts for positive benefits to the consumer and healthy organizational performance.

6. Conclusion

The overall research analysis finds an effective E-supply chain and information security due to the early recognition of SC risks on supply. Risks should be considered as part of the overall supply chain management plan. The conventional sources of supply chain risk are diminished. However, with information technology solutions that enable information security, the targeted logistics and distribution industry are increasingly exposed to information technology risk due to cooperation throughout the supply chain. The supply chain might be less able to meet consumer demand in the future due to information technology-specific attacks that could take advantage of any flaws in the system. To prevent such losses, early supply chain screening is recommended, including:

- Leveraging the "PPRR" (Prevention, Preparedness, Response & Recovery) risk management model
- Environmental Risk management
- Improving Cyber SC risk management
- Tracking the right freight carrier metric
- Implementing logistics contingency plan
- Internal risk awareness training sessions
- Consolidating data with easy access (ecosystem Software)

Even though a prevailing review of this research considers cooperation and integration beneficial to supply chain management, the benefit of IT integration must be weighed against the risks posed by information security flaws.

7. Recommendation and limitations

There are some limitations in the research. First, the targeted industry assessed is limited to the specific area. Thus, future research should incorporate extensive geographical location. Second, the mediating effect of supply chain risk was examined. Therefore, future studies are recommended to investigate the brief risk prevention techniques' effects on the supply chain. However, further study into other areas can be carried out utilizing the risk categories and summary results provided in this research. To manage supply chain risks more effectively, researchers are expected to gain from this literature review for future studies.

References

Attaran, M. (2007). RFID: an enabler of supply chain operations. *Supply Chain Management: An International Journal, 12*(4).

Aloqool, A., Alharafsheh, M., Abdellatif, H., Alghasawneh, L. A. S., & Al-Gasawneh, J. A. (2022). The mediating role of customer relationship management between e-supply chain management and competitive advantage. *International Journal of Data and Network Science*, *6*(1), 263–272. https://doi.org/10.5267/J.IJDNS.2021.9.002

Alshurideh, M. T., Al Kurdi, B., Alzoubi, H. M., Ghazal, T. M., Said, R. A., AlHamad, A. Q., Hamadneh, S., Sahawneh, N., & Al-kassem, A. H. (2022). Fuzzy assisted human resource management for supply chain management issues. *Annals of Operations Research*, 1–19.

Angerhofer, B. J., & Angelides, M. C. (2006). A model and a performance measurement system for collaborative supply chains. *Decision Support Systems*, *42*(1), 283–301.

Baabdullah, A. M., Alalwan, A. A., Rana, N. P., Shraah, A. Al, Kizgin, H., & Patil, P. P. (2019). Mobile App Stores from the User's Perspective. *International Working Conference on Transfer and Diffusion of IT*, 21–30.

Bolhari, A. (2009). Electronic-supply chain information security: A framework for information security in e-SCM (e-SCIS). *Proceedings of the 7th Australian Information Security Management Conference*, *December*, 72–81.

Can Saglam, Y., Yildiz Çankaya, S., & Sezen, B. (2020). Proactive risk mitigation strategies and supply chain risk management performance: an empirical analysis for manufacturing firms in Turkey. *Journal of Manufacturing Technology Management*, *32*(6), 1224–1244. https://doi.org/10.1108/JMTM-08-2019-0299

Cheung, K. F., Bell, M. G. H., & Bhattacharjya, J. (2021). Cybersecurity in logistics and supply chain management: An overview and future research directions. *Transportation Research Part E: Logistics and Transportation Review*, *146*(July 2020), 102217. https://doi.org/10.1016/j.tre.2020.102217

Chu, C. Y., Park, K., & Kremer, G. E. (2020). A global supply chain risk management framework: An application of text-mining to identify region-specific supply chain risks. *Advanced Engineering Informatics*, *45*(August 2019), 101053.

Demeter, K., & Gelei, A. (2004). Supply chain management framework : dimensions and development stages. *Supply Chain*

Management, *June*, 15–24.
Falasca, M., Zobel, C. W., & Cook, D. (2008, May). A decision support framework to assess supply chain resilience. In *Proceedings of the 5th International ISCRAM Conference* (pp. 596-605).
Gölgeci, I., & Ponomarov, S. Y. (2015). How does firm innovativeness enable supply chain resilience? The moderating role of supply uncertainty and interdependence. *Technology Analysis & Strategic Management*, *27*(3), 267-282.
Gurtu, A., & Johny, J. (2021). Supply chain risk management: Literature review. *Risks*, *9*(1), 1–16.
Hamadneh, Samer, Pedersen, O., & Al Kurdi, B. (2021). An Investigation of the Role of Supply Chain Visibility into the Scottish Bood Supply Chain. *Journal of Legal, Ethical and Regulatory Issues*, *24*(Special Issue 1), 1–12.
Heckmann, I., Comes, T., & Nickel, S. (2015). A critical review on supply chain risk–Definition, measure and modeling. *Omega*, *52*, 119–132.
Hunitie, M. F., Saraireh, S., Al-Srehan, H. S., Al-Quran, A. Z., & Alneimat, S. (2022). Ecotourism Intention in Jordan: The Role of Ecotourism Attitude, Ecotourism Interest, and Destination Image. *Information Sciences Letter: An International Journal*, *11*(5), 1815–1822.
Joghee, S., Alzoubi, H. M., Alshurideh, M., & Al Kurdi, B. (2021). The Role of Business Intelligence Systems on Green Supply Chain Management: Empirical Analysis of FMCG in the UAE. *The International Conference on Artificial Intelligence and Computer Vision*, 539–552.
Kumar, A., Garg, R., & Garg, D. (2020). Development of a Structural Model of Risk Factors involved in E-Supply chain adoption in Indian Mechanical Industries. *International Journal of Supply and Operations Management*, *7*(3), 242–260.
Kumar, A., Garg, R. K., & Garg, D. (2019). An empirical study to identify and develop constructive model of e-supply chain risks based on indian mechanical manufacturing industries. *Management Science Letters*, *9*(2), 217–228.
Kunnathur, A., & Vaithianathan, S. (2008). Information Security Issues In Global Supply Chain. *Utoledo.Edu*, 1–32.
Kurdi, B., Alzoubi, H., Akour, I., & Alshurideh, M. (2022). The effect of blockchain and smart inventory system on supply chain performance: Empirical evidence from retail industry. *Uncertain Supply Chain Management*, *10*(4), 1111–1116.
Lee, K., Azmi, N., Hanaysha, J. R., & Alzoubi, H. M. (2022a). The effect of digital supply chain on organizational performance: An empirical study in Malaysia manufacturing industry. *Uncertain Supply Chain Management*, *10*(2), 495–510.
Lee, K., Romzi, P., Hanaysha, J., Alzoubi, H., & Alshurideh, M. (2022b). Investigating the impact of benefits and challenges of IOT adoption on supply chain performance and organizational performance: An empirical study in Malaysia. *Uncertain Supply Chain Management*, *10*(2), 537–550.
Pettit, T. J., Croxton, K. L., & Fiksel, J. (2019). The evolution of resilience in supply chain management: a retrospective on ensuring supply chain resilience. *Journal of Business Logistics*, *40*(1), 56-65.
Pournader, M., Kach, A., & Talluri, S. (2020). A Review of the Existing and Emerging Topics in the Supply Chain Risk Management Literature. *Decision Sciences*, *51*(4), 867–919. https://doi.org/10.1111/deci.12470
Purwanto, A., Syahril, S., Rochmad, I., Fahmi, K., Syahbana, R., & Firmansyah, A. (2022). Analyzing the relationship between green innovation, creative excellence, empowerment and marketing performance of Indonesian SMEs. *Journal of Future Sustainability*, *2*(2), 53-56.
Qi, F., Abu-Rumman, A., Al Shraah, A., Muda, I., Huerta-Soto, R., Hai Yen, T. T., Abdul-Samad, Z., & Michel, M. (2022). Moving a step closer towards environmental sustainability in Asian countries: focusing on real income, urbanization, transport infrastructure, and research and development. *Economic Research-Ekonomska Istraživanja*, 1–20.
Rafati, E. (2022). The bullwhip effect in supply chains: Review of recent development. *Journal of Future Sustainability*, *2*(3), 81-84.
Rajesh, R., & Ravi, V. (2015). Modeling enablers of supply chain risk mitigation in electronic supply chains: A Grey-DEMATEL approach. *Computers and Industrial Engineering*, *87*(May 2015), 126–139.
Salloum, S. A., Alshurideh, M., Elnagar, A., & Shaalan, K. (2020). Machine Learning and Deep Learning Techniques for Cybersecurity: A Review. *Joint European-US Workshop on Applications of Invariance in Computer Vision*, 50–57.
Shamout, M., Ben-Abdallah, R., Alshurideh, M., Kurdi, A., & B., H. (2022). S. (2022). A conceptual model for the adoption of autonomous robots in supply chain and logistics industry. *Uncertain Supply Chain Management*, *10*(2), 577–592.
Sindhuja, P. N. (2014). Impact of information security initiatives on supply chain performance an empirical investigation. *Information Management and Computer Security*, *22*(5), 450–473. https://doi.org/10.1108/IMCS-05-2013-0035
Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. *Nist Special Publication*, *800*(30), 800–830.
Tarafdar, M., & Qrunfleh, S. (2017). Agile supply chain strategy and supply chain performance: complementary roles of supply chain practices and information systems capability for agility. *International Journal of Production Research*, *55*(4), 925-938.
Yang, J., Xie, H., Yu, G., & Liu, M. (2021). Antecedents and consequences of supply chain risk management capabilities: an investigation in the post-coronavirus crisis. *International Journal of Production Research*, *59*(5), 1573–1585.