

Uncertain Supply Chain Management

homepage: www.GrowingScience.com/uscm

The impact of cyber resilience and robustness on supply chain performance: Evidence from the UAE chemical industry

Muhammad Turki Alshurideh^{a,b,*}, Enass Khalil Alquqa^c, Haitham M. Alzoubi^d, Barween Al Kurdi^e and Ahmad AlHamad^f

^aDepartment of Marketing, School of Business, The University of Jordan, Amman 11942, Jordan

^bDepartment of Management, College of Business, University of Sharjah, Sharjah 27272, United Arab Emirates

^cCollege of Art, Social Sciences and Humanities, University of Fujairah, United Arab Emirates

^dSchool of Business, Skyline University College, Sharjah, United Arab Emirates

^eDepartment of Marketing, Faculty of Economics and Administrative Sciences, The Hashemite University, P.O. Box 330127, Zarqa 13133, Zarqa, Jordan

^fUniversity of Sharjah, United Arab Emirates

ABSTRACT

Article history:

Received July 5, 2022

Received in revised format

August 26, 2022

Accepted October 14 2022

Available online

October 14 2022

Keywords:

Cyber Resilience

Supply Chain Robustness

Supply Chain Performance

Chemical Industry

UAE

This paper examines the impact of cyber resilience and supply chain (SC) robustness on supply chain performance in the UAE chemical industry. No prevailing empirical evidence makes this research unique and beneficial to the literature and future research related to cyber resilience in the chemical industry. Moreover, this research is a contemporary contribution to the research of the UAE chemical industry. The study applies a quantitative approach with causal, exploratory and analytical design. The magnitude of the industry is emphasized by choosing cluster sampling techniques. Data is collected from chemical manufacturing companies located in Abu Dhabi, UAE. A valid sample of 303 participants is used for data analysis. A positive direct impact with a significant level of cyber resilience and SC robustness on supply chain performance is found. Current hypothetical model assessment in one industry limits the research findings. It is recommended that other industries be investigated through longitudinal research. A system of diverse detection and defense mechanisms is required. For the chemical industry, an effective cyber security plan would strengthen resilience against cyberattacks and improve SC performance.

© 2023 Growing Science Ltd. All rights reserved.

1. Introduction

Chemicals are virtually ubiquitous in our environment. A chemical is present in 96% of all produced products, including everything from our cars to our medications to the gadget we are reading this on. The chemical industry has been and will continue to be a significant driver of economic development domestically and internationally. However, the sector has recently been severely impacted by trade restrictions, rising levels of protectionism, and the global COVID-19 pandemic. However, with time chemical industries are facing some challenges like supply shortages, unstable raw material prices, and transportation disruptions are just some of the causes of supply chain problems in the chemical sector. Overcoming these difficulties requires a thorough and systematic approach considering the chemical sector's unique requirements. Additionally, cyber resilience refers to the group of activities, methods, and procedures needed to safeguard a company's digital assets (Aityassine et al., 2022). This includes protection against data loss, unauthorized access, and online attacks on computer networks and connected devices (Naqvi et al., 2021). Cyber security management is required for all industrial sectors that use computer technology for automation, control, and information storage (Salloum et al. 2020). Regulations exist at the

* Corresponding author

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

© 2023 Growing Science Ltd. All rights reserved.

doi: 10.5267/j.uscm.2022.10.008

local, national, and international levels to guide, oversee, and sometimes control businesses in adhering to the standards required for their operations in their respective region (Colicchia et al., 2019; El Refae et al., 2021).

The chemical supply chain is often lengthy and involves many steps, from production to delivery. This can lead to many difficulties, ranging from managing environmental concerns to ensuring product quality. Besides, due to the market's instability, prices can change quickly, making it challenging to predict demand (Alshurideh, 2022). Supply chain management is, therefore, crucial for chemical firms. They can guarantee a consistent supply of high-quality items to satisfy the needs of their clients by being aware of and addressing these difficulties (Qi et al., 2017; Alolayyan et al., 2022).

Furthermore, a robust supply chain reduces disruption that can be costly to supply firms in terms of time and money and damage their brand (Hamadneh et al., 2021a; Kurdi et al. 2022). The supply chain must be consistent for a company to perform well overall (Simchi-Levi et al., 2018). Therefore, examining the need for cyber resilience and supply chain robustness is vital to enhance the firm's overall supply chain performance. This research is mainly purposive to empirically investigate the study in the Abu Dhabi, UAE, chemical industry. It is expected that the research findings will lead to constructive outcomes and contribute to the literature and knowledge of industry researchers.

2. Theoretical framework

2.1 *Cyber Resilience in Supply Chain*

The potential impact of disruptions on a business and its supply chain emphasizes the significance of building cyber resilience (Annarelli & Palombi, 2021). The definition states that cyber resilience policies should strive to maximize these elements at four levels: timely and economically efficient preparation for a tumultuous situation, response to the event, recovery from the situation, and growth/gaining a competitive edge after the event. On the other hand, the massive scope of the COVID-19 outbreak has revealed systematic supply-chain vulnerabilities that can no longer be ignored. Thus, the perspective has changed, and the ability to recover more quickly than other companies in industries makes up for the increased investment needed (McPhee & Khan, 2015). The supply chain has always been perceived as being important (Hamadneh et al., 2021b). This is for the long-term success and efficiency of the business today (Joghee et al., 2021). When regarded in this light, the supply chain threatens any disruption in the organization's ability to operate (Alshurideh et al. 2022). Resilient supply chains are the best strategy. For instance, a company with inadequate supply chain resilience would have seen the breakdown of its worldwide supply networks and a sharp decline in profitability during the Covid-19 epidemic.

2.2 *Supply Chain Robustness*

Collaboration among a company's collaborative actions goes beyond day-to-day operations to achieve significant long-term profit (Lee et al., 2022 a&b). From the process/machine to the system and company levels, robustness has become necessary at every level of the production hierarchy. Companies are finding it increasingly difficult to absorb additional supply-side expenses as fluctuating material prices squeeze margins and the marketing effort necessary to differentiate branded goods from personal rivals rises. Suppliers collaborate to provide more than just a necessary component or service. They also work with engineers to reduce costs from buyers' and suppliers' standpoints. They may even handle the full delivery of the system from start to finish. Use collaborative research and development to co-design with R&D staff as an alternative (AlSuwaidi et al., 2021). The growing importance of supply chain collaboration necessitates an emphasis on intercompany collaboration understanding to get chain members ready to start working together successfully (Shamout, 2019). Companies can significantly boost their chances of cooperation by being more deliberate about the issues they want to work on, the suppliers/partners they choose, and how they conduct their collaboration efforts:

- Choose suppliers and partners based on their capabilities, strategic goals, and potential value.
- Collaborate in areas where you already have a solid foundation.
- Invest in the right people and infrastructure
- Create a robust, collaborative performance-management system.
- In the long run, collaborate

2.3 *Supply Chain Performance*

Performance can be defined as the accomplishment of measurable goals (AlShurideh et al., 2019). It is not only about what people accomplish but also how they accomplish it. Excellent performance results from appropriate behavior and successfully applying required knowledge, skills, and competencies. Performance management is primarily about managing expectations (Shahzad et al., 2020). Performance management needs to evaluate how results are achieved to understand what needs to be done to improve them because this gives them the data. The competitive market has become more dynamic, necessitating businesses to react quickly and make essential changes. In this battle for market participation, companies must regularly review performance indicators to determine if procedures and actions are being followed. Satisfactorily, passing it on as a competitive advantage result in a significant improvement in business profitability. Organizations focus on creating performance indicators for each business unit that are developed and used separately to measure performance. As a result, there is an impression that the KPIs are not aligned, if not at odds. Effective SC performance management is required by businesses to assist them in aligning their workers, assets, and procedures to achieve their strategic goals through formal and informal means (Caputo et al., 2004). The following presents the organization definitions.

Variables	Definition	Reference
Cyber Resilience	Business continuity, information systems security, and organizational resilience are all incorporated under the concept of “cyber resilience”.	(McPhee & Khan, 2015)
Supply Chain Robustness	Supply chain robustness, defined as the ability to deal with disruptions and interruptions both internally and externally, is becoming increasingly crucial.	(Shamout, 2019)
Supply Chain Performance	The term “supply chain performance” refers to the actions the extended supply chain takes to meet end-customer demands. This includes ensuring that products are available, that deliveries are made on time, and that the supply chain has all the inventory and capacity it needs to do so promptly.	(Zhou & Benton, 2007)

2.4 UAE Chemical Industry Description

In many nations, the chemical sector is a vital component of the national infrastructure. The energy, water, and food sectors are all equally important. The chemical and medical industries link increases the need to protect plants. As the regional and global economies are anticipated to recover after the COVID-19 outbreak, the Gulf Petrochemicals and Chemicals Association (GPCA), the voice of the chemical industry in the Arabian Gulf, stated that the chemical and petrochemical sector in the Arabian Gulf is dignified for growth in 2021–2022. The regional chemical industry is anticipated to experience growth across all key indicators, including chemical sales revenue, production output, and international trade, on the back of an increase in regional economic activity, supported by a swift vaccination roll-out and the global economic recovery. The GCC chemical sector has approximately USD 71 billion in planned and committed investments for 2020 to 2024, despite significant decreases in worldwide investment. There are worries, too, that regional petrochemical firms may wait to add additional capacity before the market for chemical goods fully recovers.

3. Literature review

3.1 Relationship and Impact of Cyber Resilience on Supply Chain Performance

Cyber resilience strategy plays a vital role in supply chain performance. Cyber resilience strategy is the ability of a company or business to grow in adverse conditions, such as in the face of a financial crisis, unknown risks, and challenges. Cyber resilience plays a vital role in sustaining organizational performance. Sustainable performance implies the ability of an organization to fulfil all the requirements of the customers and stakeholders by balancing all kinds of management. Thus, the Cyber resilience strategy strongly impacts sustainable performance (Durach et al., 2015). As a result, cyber resilience works on maintaining all cyber issues by solving all problems that arise while working in the cyber. The main benefit of cyber resilience is to minimize the cyberattacks or the cyber threats of the organizations that the complex company faces in adverse situations and precarious circumstances. Cyber resilience is the strategy that enables organizations to overcome the risk and withstand the complex situations the company going through to recover from cyber risks (Wolden et al., 2015). Globally, technological progress, tough competition, high complexities inside the demand market, and a volatile economic climate enhance the possibility of hazards and interruptions, causing extra costs for businesses, suppliers and distributors, and the market. Reorganizing supply chain functions to mitigate risks from the volatile and uncertain business environment could amplify the severity of supply chain interruptions. Identifying and measuring supply chain risks necessitate high-complexity risk management approaches that result in effective market shock reactions (Urciuoli, 2015). Supply chain resiliency is a prevalent issue in modern supply chain research. Knowing where this concept fits into the supply chain management research makes the difference in the role of supply chain response to market demands and overall organizational competitiveness. Supply chain resilience requires knowledge of reactive capability and post-disruption actions. Supply chain resilience necessitates reengineering distribution network operations and activities, collaboration among supply chain stakeholders, supply chain agility, speed in the supply chain function, and creating a risk mitigation mindset in the business. Based on previous studies, organizations are becoming more aware of supply chain issues. Global businesses and societies rely heavily on supply chains (Bahrami & Shokouhyar, 2021). A hypothesis has been developed for current research based on evidence from the literature.

H₁: *Cyber resilience has a significant impact on supply chain performance.*

3.2 Relationship and Impact of Robustness on Supply Chain Performance

Cyber resilience strategy and sustainable performance are related similarly to supply chain robustness and cyber resilience. A company's ability to recover from or otherwise handle any problems that arise while working on cyber-related projects is known as cyber resilience (Shamout, 2019). Supply chain robustness is the ability to ensure that a product will be available as often as feasible, at the lowest possible cost, with the highest level of customer satisfaction, and on schedule. These are some of the aspects that the supply chain relies on. In this situation, cyber resilience can benefit an organization's expansion and development by ensuring a steady supply of goods (Monostori, 2018). Cyberattacks or cyber threats occasionally create corporation challenges during its robust supply chain of productivity. A robust supply chain of productivity is a very significant and demanding undertaking (Rahim et al., 2021). A company can take the help of a cyber resilience strategy for its robust product supply. Nowadays, robust chain supply develops daily, and its popularity is also increasing. According to Chen Dui & Zhang (2020), sometimes the company faces various risks in its productivity and supply, availability, etc., and sometimes it can find the help of cyber resilience; thus, this issue can be overridden. Cyber resilience strategy plays an essential role in the supply chain of products by ensuring the continuity of the business to avoid issues faced by the organization. Sometimes the company faces supply chain issues created by human or other cyber threats (Colicchia et al.,

2019). Thus, solving the issues that arise from cyber threats cannot be ignored and solved with a cyber resilience strategy. Therefore, cyber resilience significantly impacts supply chain robustness, which is related. Based on proven relationship statements, a hypothesis has been developed for the current research supporting literature.

H₂: *Supply chain robustness has a significant impact on supply chain performance.*

3.3 Relationship and Impact of Cyber Resilience & Robustness on Supply Chain Performance

According to Di Vaio and Varriale (2020), a cyber resilience strategy is essential for solving all cyber threats and issues. For better performance and a robust supply chain, an organization or company needs to work on cyber resilience. A cyber resilience strategy is one of the methods through which a company can easily recover and override various cyber issues. Sometimes, these issues could be so effective for the organizations that the company may face various issues such as failure to meet the customers' expectations, loss of money with abandoned profit, low productivity etc. Based on previous studies, a company should act on the cyber resilience strategy harmoniously without affecting the growth and development of the company in terms of its productivity, customer review and profits (Gawankar et al., 2019). Nowadays, the supply chain has gained much popularity. However, supply chain robustness sometimes faces various issues caused by human factors or cyber threats. With the help of supply chain performance, a company could easily achieve a supply chain by fulfilling all kinds of requirements of the customers harmoniously. It is the only method the organization can apply to harmoniously manage all kinds of requirements (Allaoui et al., 2019). Therefore, both sustainable performance and supply chain robustness are related. As discussed above, an organization's confidential information can be protected through cyber resilience. Cyber resilient organizations tend to fight back quickly against known and unknown threats, advertise, and face challenges to improve the organization. This protects the organization from cyber-attacks and data breaches and maintains system hygiene.

The risks are later minimized or transferred by creating a plan to outline exactly how much risk the cyberattack has based on the knowledge gathered (Kumar, 2021). After identifying a reliable worldwide supply chain in cyberspace within the network offers cyber insurance. When the supply chain functions optimally, data, money, and products are exchanged at the ideal time, amount, location, and quality (Urciuoli, 2015). The supply chain networks require cyber resilience for proper and efficient exchange. In order for a company to be resilient, the following steps can be taken:

- Diversifying the supply chain networks
- Having open and direct conversations with the supplier networks about what to expect
- Identifying weaknesses and redundancy in the supply chain.
- Distributing physical stocks across various locations.
- Keeping "safety stocks" to avoid shortages in the future.

Based on the implications of resilient cyber strategies, supply chain networks can quickly bounce back from disruptions caused by situations such as terrorist attacks, pandemics, natural disasters, etc. When dealing with uncertain situations and desired performances, flexibility, visibility, collaboration, and responsiveness can be used more quickly (Taghavi et al., 2021). Resilient supply chains that can withstand such shock via transparency, rapidity, adaptability, and cooperation are crucial because supply chain failures occur frequently and have a large impact that adds to the existing body of research on supply chain collaboration and resilience. The above literature supports the hypothesis developed for current research.

H₃: *Cyber resilience and supply chain robustness significantly impact supply chain performance.*

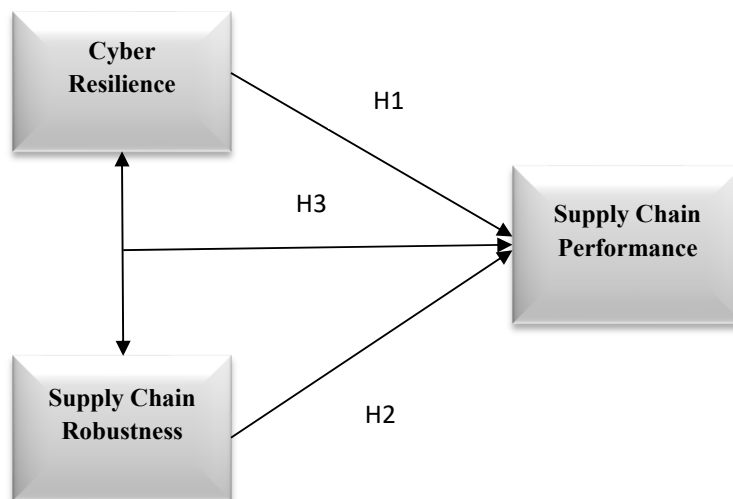


Fig. 1. Research Model

3.4 Problem Statement & Research Gab

To fill the gap identified by the previous studies, the impact of cyber resilience and SC robustness is proposed to measure SC performance. Supply chain collaboration allows growing interactions, enables collaborative efforts, and inspires real-time information exchange; thus, all are necessary for formulating, reacting, and recovering from supply disruptions when dealing with cyber security threats and strategies (Shamout, 2019). Therefore, this research explores cyber resilience, robustness and SC performance with literature and mainly supplements empirical evidence from the UAE chemical industry. Fig. 1 shows the research model.

3.5 Research Methodology and Design

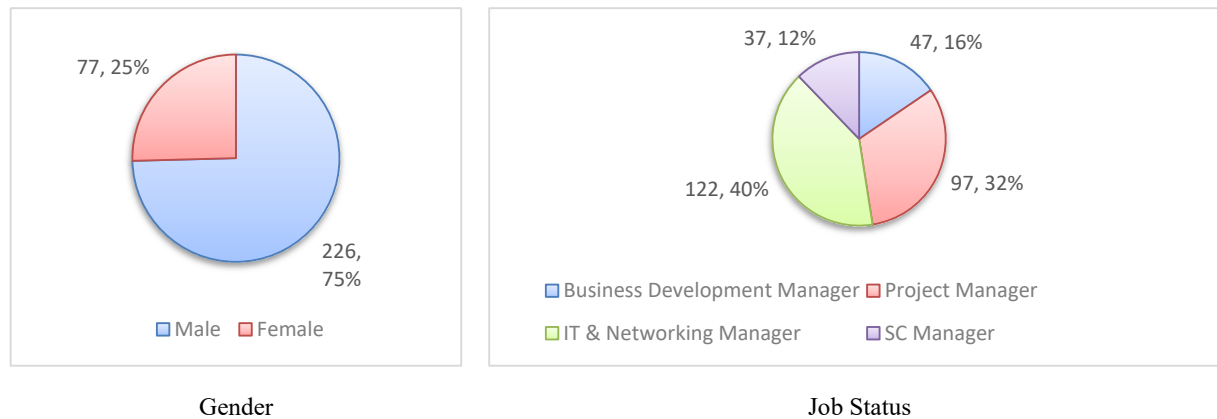
The exploration of identified constructs enabled us to empirically investigate the supply chain performance, cyber resilience and supply chain robustness. The research variables were assessed using quantitative techniques using causal, exploratory and analytical research. To collect data, an online questionnaire was developed and sent online via email. The hypothesis was tested through regression analysis using ANOVA.

3.6 Population, Sample & Unit of Analysis

The UAE Chemical Industry was the target population of the research. A total of 88 chemical manufacturing companies were assessed to gather data. Eight hundred questionnaires were emailed to the correspondents, and a sample of 303 was utilized after data screening. The questionnaire was developed using a Five Point Likert scale with 23 items. The items were classified based on the variables as 7 items were used to assess Cyber Resilience, 9 items were used to evaluate Supply chain robustness, and 7 items were used to evaluate supply chain performance.

4. Data analysis ATA ANALYSIS

Fig. 2 presents personal characteristics of the participants.



4.1 Reliability, Descriptive & Correlation

The data exploration for the reliability analysis showed a high level of reliability through Cronbach's Alpha test. The cyber resilience's reliability was $.83$, $.86$ for SC Robustness & $.87$ for SC performance. Table 1 explains the descriptive analysis with the mean value for cyber resilience as $M=2.71$ & $SD=74\%$ extent to agreeableness, mean value for SC Robustness $=3.06$ & $SD=60\%$. Supply chain performance mean identifies $=2.83$ with $SD=80\%$. The correlation results are also shown in table 2. There is a high correlation between cyber resilience and SC Robustness $r=.76$, $P<0.05$ at the significance level. SC robustness and SC performance are highly correlated with a significant value of $r=.84$, $P<0.05$. Finally, the relationship between cyber resilience and SC performance is also depicted as highly correlated and positively significant $r=.85$, $P<0.05$, respectively. Table 2 also presents the summary of the regression analysis for testing the hypotheses of the survey.

Table 1

Reliability analysis, descriptive stats & Correlation coefficients

Construct	No. of items	Cronbach's Alpha	Mean	S.D	Cyber Resilience	SC Robustness	Supply Chain Performance
Cyber Resilience	7	.83	2.71	0.74	1		
SC Robustness	9	.86	3.06	0.60	.764	1	
Supply Chain Performance	7	.87	2.83	0.80	.852	.848	1

Intelligent Information System ($M=2.15$, $SD=52\%$), Cyber Resilience ($M=3.05$, $SD=58\%$), E-Supply Chain $M=2.48$, $SD=45\%$. -Level of significance at $P<0.05^{**}$

Table 2
Linear Regression, Hypothesis testing using ANOVA

Hypothesis	Construct Relationship	β	R ²	Adjusted R ²	p-value	t-value	Hypothesis Supported
H ₁	CR→SCP	.852	.726	.726	.000	12.99	Yes
H ₂	ROB→SCP	.842	.710	.709	.000	11.91	Yes
H ₃	CR*ROB→SCP	.902	.814	.813	.000	2.45	Yes

Dependent variable= Supply Chain Performance, Independent Variable=Cyber Resilience & Robustness, *Level of Significance ($\alpha \leq 0.05$)

**Critical t-value (df/p) = 1.64

4. Discussion

It has been validated by the statistical analysis that developed hypothesis 1 designated as positively significant, which demonstrated the relationship between Cyber Resilience and Supply chain performance $\beta=.85$, $t=12.99$, & $R^2=.72$, indicating 72% variance in the construct. Thus, H1 is supported by this analysis. For the second hypothesis, the relationship between supply chain robustness and supply chain performance is measured as positive and significant, illustrated in Table 3 as: $\beta=.84$, $t=11.91$, & $R^2=.71$, and the variance noted as 71% in the variables with positive critical value and significance level $P<0.05$. H2 is also accepted. The impact of cyber resilience and SC robustness on supply chain performance demonstrate a positive significant association $\beta=.90$, $t=2.45$, & $R^2=.81$. It has been acknowledged that the significant association of the proposed construct validates the hypothesis developed in the current research. Based on the statistical results, H3 is also accepted.

5. Conclusion

The supply chain has been found to play an essential role in an organization. These research findings emphasize the acquisition of cyber resilience to improve supply chain performance, reduce cost, make operations more efficient, prevent reputational harm, and reduce financial losses. A resilient supply chain reduces unrest, strengthens transactional relationships, diversifies the supply chain, and balances resiliency and flexibility with cost-effectiveness. Therefore, chemical sector supply chains face pressure to keep pace with the latest technological advances while adhering to environmental requirements. The supply chain is already exposed to risks that cannot be eliminated but can be managed efficiently. Additionally, these research findings may encourage chemical industrialists to take advantage of technological advances to be competitive and profitable.

6. Recommendation and limitations

The overall research was completed with some limitations, including the lack of previous research on the proposed hypothetical model in the selected industry. It is recommended for future research to revise the model in other industries with more supply chain disruption strategies, including segmentation, regionalization, and supply chain diversity, while implementing technological advantages. Second, this research was conducted over a shorter period. Thus, for clearer results, it is recommended that future research be conducted longitudinally.

References

- Aityassine, F., Soumadi, M., Aldiabat, B., Al-Shorman, H., Akour, I., Alshurideh, M., & Al-Hawary, S. (2022). The effect of supply chain resilience on supply chain performance of chemical industrial companies. *Uncertain Supply Chain Management*, 10(4), 1271–1278.
- Allaoui, H., Guo, Y., & Sarkis, J. (2019). Decision support for collaboration planning in sustainable supply chains. *Journal of Cleaner Production*, 229, 761–774. <https://doi.org/10.1016/j.jclepro.2019.04.367>
- Alolayyan, M., Al-Rwaidan, R., Hamadneh, S., Ahmad, A., AlHamad, A., Al-Hawary, S., & Alshurideh, M. (2022). The mediating role of operational Flexibility on the relationship between quality of health information technology and management capability. *Uncertain Supply Chain Management*, 10(4), 1131–1140.
- AlShurideh, M., Alsharari, N. M., & Al Kurdi, B. (2019). Supply Chain Integration and Customer Relationship Management in the Airline Logistics. *Theoretical Economics Letters*, 9(02), 392–414.
- AlSuwaidi, S. R., Alshurideh, M., Al Kurdi, B., & Aburayya, A. (2021). The Main Catalysts for Collaborative R&D Projects in Dubai Industrial Sector. *The International Conference on Artificial Intelligence and Computer Vision*, 795–806.
- Annarelli, A., & Palombi, G. (2021). Digitalization capabilities for sustainable cyber resilience: a conceptual framework. *Sustainability (Switzerland)*, 13(23). <https://doi.org/10.3390/su132313065>
- Bahrami, M., & Shokouhyar, S. (2021). The role of big data analytics capabilities in bolstering supply chain resilience and firm performance: a dynamic capability view. *Information Technology and People*, September 2021. <https://doi.org/10.1108/ITP-01-2021-0048>
- Caputo, A. C., Cucchiella, F., Fratocchi, L., Pelagagge, P. M., & Scacchia, F. (2004). Analysis and evaluation of e-supply chain performances. *Industrial Management and Data Systems*, 104(7), 546–557.

- <https://doi.org/10.1108/02635570410550214>
- Colicchia, C., Creazza, A., & Menachof, D. A. (2019). Managing cyber and information risks in supply chains: insights from an exploratory analysis. *Supply Chain Management*, 24(2), 215–240. <https://doi.org/10.1108/SCM-09-2017-0289>
- Di Vaio, A., & Variiale, L. (2020). Blockchain technology in supply chain management for sustainable performance: Evidence from the airport industry. *International Journal of Information Management*, 52, 102014.
- Durach, C. F., Wieland, A., & Machuca, J. A. D. (2015). Antecedents and dimensions of supply chain robustness: A systematic literature review. *International Journal of Physical Distribution and Logistics Management*, 45, 118–137. <https://doi.org/10.1108/IJPDLM-05-2013-0133>
- El Refae, G., Nuseir, M., & Alshurideh, M. (2021). The influence of social media regulations boundary on marketing and commerce of industries in UAE. *Journal of Legal, Ethical and Regulatory Issues*, 24(Special Issue 6), 1–14.
- Gawankar, S. A., Gunasekaran, A., & Kamble, S. (2019). A study on investments in the big data-driven supply chain , performance measures and organisational performance in Indian retail 4 . 0 context. *International Journal of Production Research*, 0(0), 1–20. <https://doi.org/10.1080/00207543.2019.1668070>
- Hamadneh, S., Keskin, E., Alshurideh, M., Al-Masri, Y., & Kurdi, B. (2021a). The benefits and challenges of RFID technology implementation in supply chain: A case study from the Turkish construction sector. *Uncertain Supply Chain Management*, 9(4), 1071–1080.
- Hamadneh, Samer, Pedersen, O., & Al Kurdi, B. (2021b). 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.
- 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. (2021). Analysing the drivers of customer happiness at authorized workshops and improving retention. *Journal of Retailing and Consumer Services*, 62(January), 102619. <https://doi.org/10.1016/j.jretconser.2021.102619>
- 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.
- McPhee, C., & Khan, O. (2015). Editorial: Cyber-Resilience in Supply Chains (April 2015). *Technology Innovation Management Review*, 5(4), 3–5. <https://doi.org/10.22215/timreview/884>
- Monostori, J. (2018). Supply chains robustness: Challenges and opportunities. *Procedia CIRP*, 67, 110–115. <https://doi.org/10.1016/j.procir.2017.12.185>
- Naqvi, R., Soomro, T. R., Alzoubi, H. M., Ghazal, T. M., & Alshurideh, M. T. (2021). The Nexus Between Big Data and Decision-Making: A Study of Big Data Techniques and Technologies. *The International Conference on Artificial Intelligence and Computer Vision*, 838–853.
- Qi, Y., Huo, B., Wang, Z., & Yeung, H. Y. J. (2017). The impact of operations and supply chain strategies on integration and performance. *International Journal of Production Economics*, 185, 162–174. <https://doi.org/10.1016/j.ijpe.2016.12.028>
- Rahim, M. A., Rahman, M. A., Rahman, M. M., Asyhari, A. T., Bhuiyan, M. Z. A., & Ramasamy, D. (2021). Evolution of IoT-enabled connectivity and applications in automotive industry: A review. *Vehicular Communications*, 27, 100285. <https://doi.org/10.1016/j.vehcom.2020.100285>
- 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.
- Shahzad, F., Du, J., Khan, I., Shahbaz, M., & Murad, M. (2020). Untangling the influence of organizational compatibility on green supply chain management efforts to boost organizational performance through information technology capabilities. *Journal of Cleaner Production*, 266, 122029. <https://doi.org/10.1016/j.jclepro.2020.122029>
- Shamout, M. D. (2019). Does supply chain analytics enhance supply chain innovation and robustness capability? *Organizacija*, 52(2), 95–106. <https://doi.org/10.2478/orga-2019-0007>
- Simchi-Levi, D., Wang, H., & Wei, Y. (2018). Increasing Supply Chain Robustness through Process Flexibility and Inventory. *Production and Operations Management*, 27(8), 1476–1491. <https://doi.org/10.1111/poms.12887>
- Taghavi, E., Fallahpour, A., Wong, K. Y., & Amirali Hoseini, S. (2021). Identifying and prioritizing the effective factors in the implementation of green supply chain management in the construction industry. *Sustainable Operations and Computers*, 2(February), 97–106. <https://doi.org/10.1016/j.susoc.2021.05.003>
- Urciuoli, L. (2015). Cyber-Resilience: A Strategic Approach for Supply Chain Management. *Technology Innovation Management Review*, 5(4), 13–18. <https://doi.org/10.22215/timreview886>
- Wolden, M., Valverde, R., & Talla, M. (2015). The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management system. *IFAC-PapersOnLine*, 28(3), 1846–1852. <https://doi.org/10.1016/j.ifacol.2015.06.355>
- Zhou, H., & Benton, W. C. (2007). Supply chain practice and information sharing. *Journal of Operations Management*, 25(6), 1348–1365. <https://doi.org/10.1016/j.jom.2007.01.009>



© 2023 by the authors; licensee Growing Science, Canada. This is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) license (<http://creativecommons.org/licenses/by/4.0/>).