.

Impacts of Cyber Security and Supply Chain Risk on Digital Operations.

Del Giorgio Solfa, Federico.

IMPACTS OF CYBER SECURITY AND SUPPLY CHAIN RISK ON DIGITAL OPERATIONS: EVIDENCE FROM THE UAE PHARMACEUTICAL INDUSTRY

Federico Del Giorgio Solfa

Professor of Project Management at the National University of La Plata (UNLP); and Researcher at the Scientific Research at Commission of Buenos Aires Province (CIC-PBA), Argentina

ORCID: 0000-0002-0962-531X

delgiorgio@fba.unlp.edu.ar

ABSTRACT

The research explored empirical evidence to assess the impact of cyber security and supply chain risk on digital operations in the UAE pharmaceutical industry. Based on responses from 243 personnel working at 14 pharmaceutical manufacturing companies in Dubai, data were examined for normality, instrument validity and regression analysis. Cyber security and SC risk on digital operations were explored by applying convenient sampling and descriptive and analytical research design. The findings validated the significant positive association between cyber security and supply chain risk with digital operations. The research model was developed with three variables evaluated only on the pharmaceutical industry in Dubai. Future research should focus on multiple manufacturing industries by covering a larger geographic area. When suppliers are highly concentrated, customer-focused organizations with uncertain levels of digital transformation could improve their ability to manage supply chain risk by diversifying their clients. Pharmaceutical firms may require a greater focus on technology-based manufacturing firms to build and maintain customer trust. To illustrate how the pharmaceutical industry has explored the relationship between cyber security, supply chain risk and digital operations, the research highlights the significant and convoluted consequences of the relationship model that have not been previously considered.

Keywords: Cyber Security, Supply Chain Risk, Digital Operations, UAE Pharmaceutical Industry.

1. INTRODUCTION

The Internet has played a significant role in international communication for over 20 years and has become an integral part of people's daily lives. The availability, usage, and performance of the Internet have substantially improved due to innovations and low costs in this sector. The estimated number of users of the Internet is 3 billion globally. The increasing use of the Internet has increased security risks. Therefore, the issue of computer security has been around for decades and

is as old as computers [1]. As the access to a computing resource evolved from an individual to a resource distributed across a network, it became important to talk about computer security. IT security issues can affect any network architecture, from peer-to-peer to client-server. The term "cybersecurity" has recently been used to describe the collection of practices and approaches used to protect electronic systems, networks, computers, servers, mobile devices, and data from malicious intrusions [2].

The supply chain risk also exists while dealing with cyber security risks. Additionally, as people became increasingly aware of the effects of sustainable goals, sustainable supply chain management became important [3]. The supply chain of the organization was subject to greater uncertainties and threats due to increasing competition, the effects of globalization, the diversity of technical solutions, and limitless client demands [4].

The organization benefits in multiple ways from sustainable supply chain risk management, including avoiding resource consumption and cutting costs by identifying safeguards, responding quickly to an unexpected event, satisfying customers, and ensuring the successful continuity of the business [5]. All this is possible with digitization and digital operations in the firm. Digital operations are the main concern for most manufacturing organizations and their supply chains. Many people are suffering from the transition and feel overwhelmed, often approaching it primarily from a technological perspective [6].

The advent of digital operations compels us to think about how pharmaceutical operations and regulations can change in a fully digital and autonomous production environment. Digitalization, automation, and real-time data integration will lead to new operational paradigms that should enable pharmaceutical manufacturing to achieve better than six sigma quality for both small and large-molecule pharma products [7]. Therefore, this research examines the impact of cyber security and supply chain risk on digital operations [8]. Three constructs were proposed to measure the relationship between the independent and dependent variables. The impact of cyber security and supply chain risk needs to be identified by examining the relationship with digital operations in the UAE pharmaceutical manufacturing industry [9].

2. THEORETICAL FRAMEWORK

2.1 Cyber Security

It is the application of technological methods and controls to protect systems, networks, programs, devices, and information, besides building a shield for the confidentiality, integrity, and availableness of laptop systems from cyber-attacks or unauthorized access [10]. Here we aim to minimize the risk of cyber-attacks and protect systems, technologies and networks from illegal use

[11]. In addition, it protects all structure resources from external and internal attacks and natural disaster-related distractions [12]. Since the structure consists of several different systems, a good and proficient cyber security position requires organized measures for all information systems of the organization. Thus, cyber security is composed of different sub-domains, which include:

- *Network security*
- *Cloud security*
- *Identity Management & Data Security*
- *Mobile security*
- *Application security*
- *User education*

Based on current trends, the rate of cyberattacks is not slowing down. Every day, hackers are targeting businesses large and small, hoping to gain access to critical data or disrupt services [13]. The sensitive user data of these organizations is gone, causing lasting harm to their finances and reputations [14]. The changing technological world makes implementing an effective cyber security plan challenging. With updates and alterations, the software is constantly changing, creating new flaws and weaknesses, and making it susceptible to numerous cyber-attacks [15].

2.2 Supply Chain Risk

The technique of identifying, studying, and managing risks in an organization's supply chain is called supply chain risk management (SCRM). It implements worldwide supply chain risk management approaches that enable Associates in the Nursing business to run more quickly, save costs, and improve the customer experience. Supply chain management indicates how enterprises succeed in running their products and all the procedures used to transform raw materials into finished goods or services [16]. It contains devising and implementing sourcing, transformation, procurement, and supply management strategies. One of the most common ways businesses use international supply chain management methods is to boost their competitive edge. However, the globalization of supply chains risks compromising the value, safety, and endurance of the business and brand reputation. These issues also need to be considered [17].

If anything threatens a company's financial health, such as increasing part prices eating into profit margins, the company may see a monetary threat in the supply chain. If a vendor engages in destructive behavior, such as crime, child labor, or something that reflects adversely on the firm, the company's image may be at risk [18]. Of course, a supplier's social media behavior might be detrimental to a business [19]. Artificial intelligence and sophisticated analytics in various tools

allow the creation of more accurate forecasts about the availability of offers, supply bottlenecks, and related issues. Thanks to these insights, one can identify threats early on before they become a serious issue [20].

2.3 Digital Operations

Digital Operations is the idea of blending corporate procedures with ease and automation to make operational models that please customers and boost performance. A firm's most crucial business activities are controlled, re-engineered [21], updated, and carried out through digital operations to reduce operational costs, enhance user experiences, offer better results, and achieve top-line growth [22]. A company can establish more practical operational models and achieve method excellence by creating automated, data-driven platforms and trade utilities. To ensure the best digital involvement, the Digital Operations Manager is liable for the entire digital platform's stability and accessibility (counting the administration of our vendors and allies) [23]. The Digital Operations crew also controls the processes and actions that lead to changes on these platforms to minimize incidents and operational risks while maintaining the ease required to be first in the market [24].

Nowadays, the digital economy offers a brand-new opportunity to explore and develop advanced new goods, services, and practices tailored to changing consumer demands. On the other hand, old-fashioned operational models stymie a company's transformation efforts, limiting its capacity to keep pace with customer and market expectations [25]. Only corporations built on flexible, digitally, and smart connected processes can provide additional humanized transactions and practices that surpass clients' expectations [24]. Digital operations may help businesses rethink and create digital ways to improve performance and bridge method gaps between customers, dealers, and partners using method platforms, automation, and intelligence.

2.4 Operational Definitions

Variables	Definition	Reference
Cyber Security	*Cybersecurity protects internet-connected systems, including their hardware, software, and data, from cyber-attacks. This method prevents unauthorized access to data centers and other digital systems by individuals and companies.*	[26]
Supply Chain Risk	*The risk of harm or compromise posed by suppliers' supply networks, products, or services, as well as those of those suppliers.*	[27]

Digital Operations	*The idea of incorporating agility, intelligence, and automation into corporate processes to provide operational models that delight consumers and boost productivity is known as "digital operations."*	[28]

2.5 UAE Pharmaceutical Manufacturing Industry

The UAE, one of the world's fastest-growing economies, has continued to build on the thriving history of its ancestors. The UAE's economy has expanded significantly since gaining independence in 1971 due to the sector-specific expansion of numerous sectors. However, the pharmaceutical industry still largely supports the UAE's GDP [29].

Between 2021 and 2025, the UAE pharmaceutical market is forecasted to expand by 27% as the government works to turn the country into a regional industry hub. As a result, the local pharmaceutical market is anticipated to triple to $4.7 billion between 2011 and 2025. The need for digitization and cyber security is becoming increasingly evident [30], necessitating research on this industry that will incorporate the significance of cyber security and supply chain risks and their impact on Digital operations in the industry [31].

3. LITERATURE REVIEW

3.1 Relationship and impact of Cyber Security on Digital Operations

Even before a global pandemic, executive teams had to work in a challenging and dynamic environment as they attempted to protect their organisations against cyberattacks without compromising their capacity for innovation and getting the most out of technology investments [32]. The public health emergency triggered by COVID-19 has highlighted the need for production methods that can adapt to rapidly changing demand and minimise reliance on human intervention. For instance, automated and robotic procedures may be required when faced with obstacles that prevent people from working closely together [33]. Previous studies investigated pharmaceutical products and some potential legal, technological, and logistical issues that must be solved if society is to fully benefit from digital operations [34]. The demand for technological factors has increased security concerns, making cyber security a module for managing security risks through digitization. Literature mentions the significance of implementing cyber security for digital operations [35].

Based on the above discussion, we develop the following hypothesis:

H_{o1}: Cybersecurity has a significant impact on digital operations

3.2 Relationship and impact of Supply Chain Risk on Digital Operations

[36] argued that supply chain risk encourages businesses to collaborate closely with key suppliers to understand the supply market and adapt supply functions to emerging technology. The advanced use of the Internet and technology enables businesses to incorporate supply chain methods with smart technology and eliminate supply chain risks by identifying security concerns.

The integration of cutting-edge manufacturing technology during the fourth industrial revolution paved the way for integrated, autonomous, and self-organizing production systems that operate without human intervention [33]. Manufacturing pharmaceuticals has been transformed by digital operations and the experiences gained in the automated and digital environment of the supply chain. Supply chain risk can be efficiently managed by applying advanced technologies to evaluate the risk factors and ways to protect against the risk. Previous studies have examined the significant impact of SC risk on digital operations [37]. Increasing supply chain resilience is key for businesses to improve their ability to respond to supply chain threats. The digital operations of businesses can help businesses increase the visibility of their supply chains and their ability to anticipate problems, enabling them to better develop risk management plans and increase supply chain resilience [38].

Based on the above discussion, we develop the following hypothesis:

H_{o2}: Supply chain risk has a significant impact on digital operations

3.3 Relationship and impact of Cyber Security and Supply Chain Risk on Digital Operations

The advent of smart gadgets and ever-changing consumer demands have accelerated global digital transformation. Consequently, firms are increasingly identifying opportunities and developing high-end capabilities to gain a competitive edge and flourish. Organizations were obliged to transition to remote work due to the epidemic, which accelerated the introduction of new technology [35]. This was where digital transformation became a reality from a long-term goal. The understanding of cyber security has changed with the increasing acceptance of digital transformation. This is due to the increase in cyberattacks, data breaches, and other incidents as the threats continue to grow, and businesses use more digital technologies across various company functions to create new business models and enhance consumer experiences [39].

Most security organizations report that their corporate executives are unaware of the harm unprotected digital assets pose to their entire portfolio. Eighty-two per cent of IT security and C-level executives reported at least one data breach following the integration of new technologies and the expansion of the supply chain, based on a Digital Transformation and Cyber Risk survey [32]. This is why the risk management function at large is so important: they design an organisation-wide cybersecurity plan that coincides with a company's objectives [40]. They must effectively

communicate to ensure that all digital assets are protected while improving cooperation at both the senior and operational levels [26].

Based on the above discussion, we develop the following hypothesis:

H_{o3}: Cyber security and supply chain risk have a significant impact on digital operations

3.4 Problem Statement & Research Gap

Previous research has demonstrated the link between digital operations and supply chain risks [36]. However, there is no evidence to support the interaction between cyber security and supply chain risk to improve or assess digital operations. Although supply chain diversity increases the risk tolerance of a supply chain, it also often leads to a more complicated supply network, which reduces the transparency of the supply chain. To manage a more complicated supply chain, digital operations can enhance the transparency of information flow through cyber security and SC activities.

3.5 General Research Model

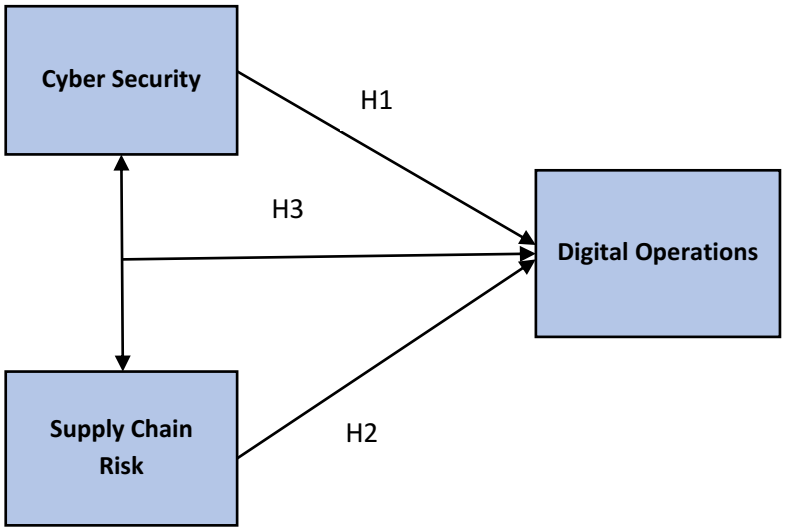

Figure1: Conceptual Research Model

3.6 Research Hypothesis

H_{O1}: Cyber Security has no statistical impact on Digital Operations in the UAE Pharmaceutical manufacturing Industry at ($\alpha \leq 0.05$) level.

H_{O2}: Supply Chain Risk has no statistical impact on Digital Operations in the UAE Pharmaceutical Manufacturing Industry at ($\alpha \leq 0.05$) level.

H_{O3}: Cyber Security and Supply Chain Risk have no statistical impact on Digital Operations in the UAE Pharmaceutical Manufacturing Industry at ($\alpha \leq 0.05$) level.

3.7 Research Methodology and Design

Descriptive and analytical research designs were used in the proposed quantitative research. A self-administered questionnaire was developed, data was gathered via an online survey for a primary purpose, and secondary data was collected by consulting scientific literature. An appropriate cluster sampling technique was used to gather data from a specified population area.

3.8 Population, Sample & Unit of Analysis

Data collected from 14 pharmaceutical companies based in Dubai, UAE, were the main sources of information from which the sample for this study was drawn. The most crucial component of this research was data collection from the employees of pharmaceutical manufacturing companies. Thus, a survey questionnaire was sent by email to 500 employees, of which 243 were used for analysis after screening. The questionnaire was developed on a five-point Likert scale (1=strongly disagree to 5=strongly agree). To assess the research variables, 25 items were used, respectively. The "Gender" and "Designation" were evaluated to obtain the demographic data.

4. DATA ANALYSIS

4.1 Demographic Analysis

To evaluate the demographic data, data were collected from male and female respondents with a high frequency of male respondents=163 and female=80. The respondents were specified by their job title, with the highest number of Manager IT & Development=78, HR manager=67, SC Officer=63 and Cyber Security Manager=35. Table 1 shows the summary of the data.

Table 1: Summary of Demographic Data

Items	Description	*f*	%
Gender	Male	163	67.1
	Female	80	32.9
Job Status	Manager IT & Development	78	32.1
	SC Officer	63	25.9
	Cyber Security Manager	35	14.4
	HR Manager	67	27.6

(N=243)

4.2 Reliability, Descriptive and Correlation

The data reliability was measured using Cronbach's5 Alpha, showing high reliability of the results. The summary of the data showed α=.89 for Cyber Security 10 items. A=.85 for Supply Chain Risk 7 items and α=.88 is for Digital Operations 8 items. Additionally, the descriptive statistics demonstrated the accepted mean and standard deviation values. M=3.12 & SD=.75 for Cyber Security. M=2.83 & SD=.68 accepted values to the benchmark for Supply Chain Risk [37]. The Mean value for Digital operations showed M=2.74 & SD=.67 as accepted values.

Table 2 illustrates the correlation coefficients depicting the relationship between Cyber Security and Supply Chain Risk r=.816 at a significance level of P<0.05**. Cyber Security and Digital Operations showed a high correlation r=.919 at a significance level of 0.05**. Finally, the correlation of Supply Chain Risk and Digital Operations was identified as highly correlated r=.842 and significant at level 0.05**. The summary of all tests is demonstrated in Table 2.

Table 2: Data Reliability, Descriptive Statistics and Correlation Coefficients

Construct	No of items	Cronbach's Alpha	Mean	SD	Cyber Security	Supply Chain Risk	Digital Operations
Cyber Security	10	.89	3.12	.75	1		
Supply Chain Risk	7	.85	2.83	.68	.816**	1	
Digital Operations	8	.88	2.74	.67	.919**	.842**	1

*Cyber Security (M=3.10, SD=74%, Supply Chain Risk (M=2.71, SD=53%), Digital Operations M=3.34, SD=69%. -Level of significance at P<0.05***

4.3 Regression Analysis and Hypothesis Testing

Table 3 illustrates the hypothesis tests for the proposed research model that shows a significant positive relationship between Cyber Security and Digital Operations β=.74, p=0.00, t=17.3, p=0.00, R^2=.845, resulting in a positive t-value and a change in relationship dependability of 84%, which is high. H1 is accepted. H2 demonstrated a significant positive relationship between Supply Chain Risk and Digital Operations β =.84, t=6.83, p=0.00, R^2=.709. A high variance showed the high dependence of SCR on Digital Operations with 70%. Thus, H2 is supported. H3 is identified with β=.933, t=2.38, p=0.00, R^2=.87 that showed a significant positive relationship and a high variance level of 87% of both variables (cyber security and supply chain risk) on Digital

Operations. Therefore, H3 is also supported in this research. Table 3 illustrate the summary of the data.

Table 3: Regression and Hypothesis Testing through ANOVA

Hypothesis	Regression Weights	Standardized Coefficients					
		β	R^2	df	Sig	t-value	Hypothesis Supported
H_1	CS→DO	.919	.845	1	.000	17.3	Yes
H_2	SCR→DO	.842	.709	242	.000	6.83	Yes
H_3	CS*SCR→DO	.933	.871	.243	.000	2.38	Yes

*Dependent Variable=Digital Operations, Independent Variable= Cyber Security & Supply Chain risk *Level of Significance ($\alpha \leq 0.05$**

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

5. DISCUSSION OF THE RESULTS

In the proposed research model, a regression analysis was performed to test the significant positive relationship between cyber security and digital operations. Our findings suggest that a strong focus on cyber security can enhance digital operations. Previous research is consistent with our findings that cyber security now offers the opportunity to digitise security risk management due to increasing security issues caused by technical elements. Implementing cyber security in digital activities enhances the work efficiency of firms [11]. The second research hypothesis has confirmed the significant positive relationship between supply chain risk and a digital operation that greatly matches previous studies [41]. Our research findings also show that businesses need to improve their ability to respond to supply chain risks by strengthening their supply chains. Businesses can improve the visibility of their supply networks and their ability to foresee issues using digital operations, which will help them develop better risk management strategies and strengthen the resilience of their supply chains [39].

The third hypothesis mentioned a positive relationship between cyber security and supply chain risk in digital operations, which verifies the findings and authenticates the previous research findings with similar findings. The understanding of cybersecurity has changed with the increasing acceptance of digital transformation. Businesses are increasingly using digital technologies in various company functions to develop new business models and improve consumer experiences to provide safe medical products, which has led to increased cyberattacks, data breaches, and other cyber disasters.

6. CONCLUSION

Based on the research findings, adopting digital processes can help control supply chain risks. Increased adoption of digital technologies can help pharmaceutical manufacturing companies share data and information more effectively, secure formulas, better manage various business processes, and predict potential risks in the future [42]. These improvements can help enhance the company's risk management and address cyber security issues. Therefore, large businesses looking to strengthen their SC resilience can organize a variety of digital improvements by aggressively implementing cyber security and putting a greater emphasis on managing supply chain risks [43].

7. RECOMMENDATIONS/LIMITATIONS

Some noted limitations of this research include the pharmaceutical manufacturing firm chosen for the research purpose limits the generalizability. However, future research can include other manufacturing firms [44]. Thus, a future perspective could use the same model to analyze the relationship in different industries and provide a more thorough explanation.

REFERENCES

[1] B. Kurdi, H. Alzoubi, I. Akour, and M. Alshurideh, "The effect of blockchain and smart inventory system on supply chain performance: Empirical evidence from retail industry," *Uncertain Supply Chain Manag.*, vol. 10, no. 4, pp. 1111–1116, 2022.

[2] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, 2021, doi: 10.1016/j.egyr.2021.08.126.

[3] M. Shamout, R. Ben-Abdallah, M. Alshurideh, A. Kurdi, and H. B., "S. (2022). A conceptual model for the adoption of autonomous robots in supply chain and logistics industry," *Uncertain Supply Chain Manag.*, vol. 10, no. 2, pp. 577–592.

[4] H. Tang, S. M. Chu, M. Hasegawa-Johnson, and T. Huang, "S:(2009)," *Emot. Recognit. from speech via Boost. Gaussian Mix. Model.*, 2009.

[5] A. Alzoubi H., A. K. M., and A. B., "K. and Ghazal, T. (2022) The effect of e-payment and online shopping on sales growth: Evidence from banking industry," *Int. J. Data Netw. Sci.*, vol. 6, no. 4, pp. 94–109.

[6] R. N. Boute and J. A. van Mieghem, "Digital Operations: Autonomous Automation and the Smart Execution of Work," *Manag. Bus. Rev.*, vol. 1, no. 1, pp. 1–19, 2021.

[7] H. M. Alzoubi, G. Ahmed, and M. Alshurideh, "An empirical investigation into the impact of product quality dimensions on improving the order-winners and customer satisfaction," *Int. J. Product. Qual. Manag.*, vol. 36, no. 2, pp. 169–186, 2022, doi: 10.1504/IJPQM.2021.10037887.

[8] Edward Probir Mondol, "the Role of Vr Games To Minimize the Obesity of Video Gamers," *Int. J. Comput. Inf. Manuf.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijcim.v2i1.70.

[9] H. M. Alzoubi, H. Elrehail, J. R. Hanaysha, A. Al-Gasaymeh, and R. Al-Adaileh, "The Role of Supply Chain Integration and Agile Practices in Improving Lead Time During the COVID-19 Crisis," *Int. J. Serv. Sci. Manag. Eng. Technol.*, vol. 13, no. 1, pp. 1–11, 2022, doi: 10.4018/IJSSMET.290348.

[10] H. M. Alzoubi, M. Alshurideh, B. A. Kurdi, I. Akour, and R. Aziz, "Does BLE technology contribute towards improving marketing strategies, customers' satisfaction and loyalty? The role of open innovation," *Int. J. Data Netw. Sci.*, vol. 6, no. 2, pp. 449–460, 2022.

[11] D. Giansanti, "Cybersecurity and the digital-health: The challenge of this millennium," *Healthc.*, vol. 9, no. 1, pp. 0–3, 2021, doi: 10.3390/healthcare9010062.

[12] Nada Ratkovic, "Improving Home Security Using Blockchain," *Int. J. Comput. Inf. Manuf.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijcim.v2i1.72.

[13] Saad Masood Butt, "Management and Treatment of Type 2 Diabetes," *Int. J. Comput. Inf. Manuf.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijcim.v2i1.71.

[14] H. M. Alzoubi, M. In'airat, and G. Ahmed, "Investigating the impact of total quality management practices and Six Sigma processes to enhance the quality and reduce the cost of quality: the case of Dubai," *Int. J. Bus. Excell.*, vol. 27, no. 1, pp. 94–109, 2022, doi: 10.1504/IJBEX.2022.123036.

[15] O. Tang and S. N. Musa, "Designing fuzzy-genetic learner model based on multi-agent systems in supply chain management," *Int. J. Prod. Econ.*, vol. 133, pp. 25–34, 2010.

[16] A. Alhamad, M. Alshurideh, K. Alomari, S. Hamouche, S. Al-Hawary, and H. M. Alzoubi, "The effect of electronic human resources management on organizational health of telecommunications companies in Jordan," *Int. J. Data Netw. Sci.*, vol. 6, no. 2, pp. 429–438, 2022.

[17] M. Alshurideh, B. Kurdi, H. Alzoubi, B. Obeidat, S. Hamadneh, and A. Ahmad, "The influence of supply chain partners' integrations on organizational performance: The moderating role of trust," *Uncertain Supply Chain Manag.*, vol. 10, no. 4, pp. 1191–1202, 2022.

[18] B. Kurdi, M. Alshurideh, I. Akour, E. Tariq, A. AlHamad, and H. Alzoubi, "The effect of social media influencers' characteristics on consumer intention and attitude toward Keto products purchase intention," *Int. J. Data Netw. Sci.*, vol. 6, no. 4, pp. 1135–1146, 2022.

[19] A. Alzoubi, "MACHINE LEARNING FOR INTELLIGENT ENERGY CONSUMPTION IN SMART HOMES," *Int. J. Comput. Inf. Manuf.*, vol. 2, no. 1, p. 2022, May 2022, doi: 10.54489/IJCIM.V2I1.75.

[20] B. Kurdi, M. Alshurideh, I. Akour, H. Alzoubi, B. Obeidat, and A. AlHamad, "The role of digital marketing channels on consumer buying decisions through eWOM in the Jordanian markets," *Int. J. Data Netw. Sci.*, vol. 6, no. 4, pp. 1175–1186, 2022.

[21] M. Farouk, "The Universal Artificial Intelligence Efforts to Face Coronavirus COVID-19," *Int. J. Comput. Inf. Manuf.*, vol. 1, no. 1, pp. 77–93, 2021.

[22] Y. Ramakrishna and H. M. Alzoubi, "Empirical Investigation of Mediating Role of Six Sigma Approach in Rationalizing the COQ in Service Organizations," *Oper. Supply Chain Manag.*, vol. 15, no. 1, pp. 122–135, 2022, doi: 10.31387/OSCM0480335.

[23] T. Eli and Lalla Aisha Sidi Hamou, "Investigating the Factors That Influence Students` Choice of English Studies As a Major: the Case of University of Nouakchott Al Aasriya, Mauritania," *Int. J. Technol. Innov. Manag.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijtim.v2i1.62.

[24] T. M. Ghazal and H. M. Alzoubi, "Fusion-based supply chain collaboration using machine learning techniques," *Intell. Autom. \& Soft Comput.*, vol. 31, no. 3, pp. 1671–1687, 2022.

[25] N. Alsharari, "the Implementation of Enterprise Resource Planning (Erp) in the United Arab Emirates: a Case of Musanada Corporation," *Int. J. Technol. Innov. Manag.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijtim.v2i1.57.

[26] A. Sutawidjaya, L. Nawangsari, and M. Maszuduylhak, "Will Digital Operations Management Improve industry 4.0?," 2020, doi: 10.4108/eai.26-11-2019.2295175.

[27] N. S. Arden, A. C. Fisher, K. Tyner, L. X. Yu, S. L. Lee, and M. Kopcha, "Industry 4.0 for pharmaceutical manufacturing: Preparing for the smart factories of the future," *Int. J. Pharm.*, vol. 602, p. 120554, 2021, doi: 10.1016/j.ijpharm.2021.120554.

[28] M. S. S. Jajja, K. A. Chatha, and S. Farooq, "Impact of supply chain risk on agility performance: Mediating role of supply chain integration," *Int. J. Prod. Econ.*, vol. 205, pp. 118–138, 2018, doi: 10.1016/j.ijpe.2018.08.032.

[29] K. L. Lee, P. N. Romzi, J. R. Hanaysha, H. M. Alzoubi, and M. Alshurideh, "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 Manag.*, vol. 10, no. 2, pp. 537–550, 2022.

[30] G. M. Qasaimeh and H. E. Jaradeh, "THE IMPACT OF ARTIFICIAL INTELLIGENCE ON THE EFFECTIVE APPLYING OF CYBER GOVERNANCE IN JORDANIAN COMMERCIAL BANKS," *Int. J. Technol. Innov. Manag.*, vol. 2, no. 1, 2022.

[31] M. Alshurideh *et al.*, "Fuzzy assisted human resource management for supply chain management issues," *Ann. Oper. Res.*, pp. 1–19, Jan. 2022, doi: 10.1007/s10479-021-04472-8.

[32] V. Mani, C. Delgado, B. T. Hazen, and P. Patel, "Mitigating supply chain risk via sustainability using big data analytics: Evidence from the manufacturing supply chain," *Sustain.*, vol. 9, no. 4, 2017, doi: 10.3390/su9040608.

[33] John Kasem and Anwar Al-Gasaymeh, "a Cointegration Analysis for the Validity of Purchasing Power Parity: Evidence From Middle East Countries," *Int. J. Technol. Innov. Manag.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijtim.v2i1.60.

[34] P. A. H. Williams, "Is Cyber Resilience in Medical Practice Security Achievable?," *Ed. Cowan Univ.*, no. August, 2010.

[35] Neyara Radwan, "the Internet'S Role in Undermining the Credibility of the Healthcare Industry," *Int. J. Comput. Inf. Manuf.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijcim.v2i1.74.

[36] W. Yin and W. Ran, "Supply Chain Diversification, Digital Transformation, and Supply Chain Resilience: Configuration Analysis Based on fsQCA," *Sustain.*, vol. 14, no. 13, 2022, doi: 10.3390/su14137690.

[37] F. D. G. Solfa, *Public Benchmarking : contributions for subnational governments and Benchmarking Design*, no. March. 2017.

[38] K. L. Lee, N. A. N. Azmi, J. R. Hanaysha, H. M. Alzoubi, and M. T. Alshurideh, "The effect of digital supply chain on organizational performance: An empirical study in Malaysia manufacturing industry," *Uncertain Supply Chain Manag.*, vol. 10, no. 2, pp. 495–510, 2022.

[39] A. Gurtu and J. Johny, "Supply chain risk management: Literature review," *Risks*, vol. 9, no. 1, pp. 1–16, 2021, doi: 10.3390/risks9010016.

[40] A. Alzoubi, "Renewable Green hydrogen energy impact on sustainability performance," *Int. J. Comput. Inf. Manuf.*, vol. 1, no. 1, pp. 94–105, 2021.

[41] A. J. Obaid, "Assessment of Smart Home Assistants as an IoT," *Int. J. Comput. Inf. Manuf.*, vol. 1, no. 1, pp. 18–38, 2021.

[42] Maged Farouk, "Studying Human Robot Interaction and Its Characteristics," *Int. J. Comput. Inf. Manuf.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijcim.v2i1.73.

[43] G. Ahmed and Nabeel Al Amiri, "the Transformational Leadership of the Founding Leaders of the United Arab Emirates: Sheikh Zayed Bin Sultan Al Nahyan and Sheikh Rashid Bin Saeed Al Maktoum," *Int. J. Technol. Innov. Manag.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijtim.v2i1.58.

[44] V. Victoria, "IMPACT OF PROCESS VISIBILITY AND WORK STRESS TO IMPROVE SERVICE QUALITY: EMPIRICAL EVIDENCE FROM DUBAI RETAIL

INDUSTRYIMPACT OF PROCESS VISIBILITY AND WORK STRESS TO IMPROVE SERVICE QUALITY: EMPIRICAL EVIDENCE FROM DUBAI RETAIL INDUSTRY," *Int. J. Technol. Innov. Manag.*, vol. 2, no. 1, 2022.