Khan, Khalid; Keramati, Abbas

Article

A framework for smart supply chain risk assessment : an empirical study

International journal of information systems and supply chain management

Provided in Cooperation with:
ZBW OAS

Reference: Khan, Khalid/Keramati, Abbas (2023). A framework for smart supply chain risk assessment : an empirical study. In: International journal of information systems and supply chain management 16 (1), S. 1 - 17.
https://www.igi-global.com/ViewTitle.aspx?TitleId=316167&isxn=9781668479148.
doi:10.4018/IJISSCM.316167.

This Version is available at:
http://hdl.handle.net/11159/652831

International Journal of Information Systems and Supply Chain Management
Volume 16 • Issue 1

A Framework for Smart Supply Chain Risk Assessment:
An Empirical Study

Khalid Khan, Toronto Metropolitan University, Canada

Abbas Keramati, State University of New York at Buffalo, USA & Toronto Metropolitan University, Canada*

ABSTRACT

This research provides a framework for assessing risks in smart supply chains using a quantitative approach. This study identifies the risk factors in smart supply chains based on an extensive literature review and interviews with professionals. By analyzing different concepts of the previous frameworks, a new one is proposed for the smart supply chain. This new framework is applied to the data collected from a survey of Canadian supply chain professionals (n = 56). The authors conducted an exploratory factor analysis to examine the construct validity of the survey results. After evaluating and assessing risks for different smart supply chain risk factors, some constructs were developed. The survey's results point to the most important risk factors for the smart supply chain, prioritized based on their high probabilities and impacts. These include risk of complexity, web application failure, talent shortage, and high-cost risk. The results also show that the most commonly implemented smart technologies in the supply chain sector are bar codes and social media.

KEYWORDS

Failure Mode and Effect Analysis (FMEA), Risk Mitigation, Risk Monitoring, Smart Supply Chain Risk Management (SSCRM), Smart Technology (ST), Supply Chain Risk Management (SCRM)

INTRODUCTION

A smart supply chain is characterized by a high degree of cyber connections enabled by sensors and electronic tools that collect big data for real-time decisions to optimize supply chain performance. The large-scale deployment of the Internet of Things (IoT) sensors and large data analytics enable preventive maintenance, avoiding disruptions from unexpected failures (Sharma et al., 2021). Likewise, the implementation of IoT, big data, and cloud computing in transport operations and infrastructure management allows for real-time route and asset optimization, improving reliability and efficiency in logistics processes. Moreover, the deployment of advanced robotics, artificial intelligence, and

DOI: 10.4018/IJISSCM.316167

*Corresponding Author

blockchain technology allow for decisions and supply chain processes to be highly automated. In contrast, the supply chain process's length is shortened through 3-D printing (Schwab, 2019).

Smart supply chain risk events represent a daily challenge to supply chains because they can cause disruptions that potentially negatively impact supply chain operations. Supply chains must effectively respond to the risk events and recover quickly to stay ahead of competitors and reduce long-term damage to their businesses. Recently, there has been an increased focus on smart supply chain risk management due to the increasing use of smart technologies, which bring many comforts and risks. Smart supply chain risk identification and assessment are important steps in smart supply chain risk management (Aqlan, 2016; Sharma et al., 2021).

Smart supply chain performance may be badly affected by the occurrence of risk events in different components and stages of the supply chain system. The management of such events is known as supply chain risk management (SCRM), an important aspect of organizational strategy. SCRM has gained more attention with the introduction of digitalization and globalization along the supply chains, and now it is called smart supply chain risk management (SSCRM; Schlüter & Henke, 2017; Sharma et al., 2020). SSCRM focuses on potential risks related to smart technologies and disruptions in the supply chain and develops mitigation strategies to minimize the impact of these disruptions and risks on smart supply chains.

An important step for risk management in a smart supply chain is understanding different risk factors and the events and conditions that drive these risks. SSCRM provides supply chain resilience by minimizing risks like cybercrimes, shortage of skilled employees, network vulnerability, data leakages, and theft of important information. The art of risk management is to identify, assess, and mitigate risks for an organization (Aqlan, 2016; Sharma et al., 2021). Based on the literature review and framework analysis of the smart supply chain and empirical research, the authors answer the following research questions:

- How does the risk management framework address risks in smart supply chains?
- To what extent are companies using smart technologies in their supply chain systems?
- What are the chances of these risks?
- What are the impacts of these risks on the organization's smart supply chain?
- How can smart supply chain risk factors be categorized?
- How can smart supply chain risks be mitigated?

After identifying and assessing the risks of supply chain management, their impact on the organization should be minimized by adopting different risk mitigation strategies (Sharma et al., 2021). An effective risk management strategy requires a comprehensive assessment of risk factors, vulnerabilities, and impacts. The survey data helps identify and assess smart supply chain risk factors and risk mitigation strategies.

LITERATURE REVIEW

Digital technologies enable people, objects, and organizations to be smart (Porter & Heppelmann, 2014) or to make autonomous and comprehensive decisions in networked contexts. Digital technologies include social media, mobile computing, analytics, and cloud computing (SMAC; Shelton, 2013; Silva et al., 2018). Additional technologies, such as augmented reality and wearables, are frequently mentioned in this context (Porter & Heppelmann, 2014). For this paper, the term smart represents all human-centered digital technologies that combine intelligence and networked collaboration to improve the performance of the supply chain processes. So, it is called a smart supply chain (SSC; Kara et al., 2020).

Following a similar logic, technical systems codes become intelligent and interconnected using digital technologies (i.e., smart technologies). Cyber-physical systems are engineered systems that communicate with each other to form the IoT; they use big data and analytics to make well-informed, local, autonomous decisions (Lee et al., 2015; Sharma et al., 2021). Lastly, smart organizations rely on similar digital technologies to integrate the system (Xu et al., 2018) by connecting partners to extended value networks (Hofmann & Rüsch, 2017). Figure 1 presents the technologies used in the SSC, and Table 1 presents the recent research on SSC risks.

Recent research on smart supply chain risk

Table 1 summarizes the literature by outlining the research objectives, research methods, and findings.

After reviewing the literature, it is clear that all of the researchers have tried identifying risk factors related to the supply chain by providing their proposed frameworks. This paper is related to their work as we are trying to find the risk factors and propose a new supply chain risk framework. However, this research is different in several ways. First, these supply chain risk factors are not traditional; instead, they are related to the smart technologies currently prevailing in the industry. Second, the latest trends in smart technologies, impact, and likelihood are determined based on the opinions of current professionals. Finally, the reduction method is applied to the survey data using exploratory factor analysis to recognize the most important and current smart supply chain risk factors. The risk factors related to the smart supply chain are presented in Table 2 with their descriptions and references.

Smart supply chain risk factors

The authors extracted some of the risk factors from the literature that may affect the SSC system, so they are called SSC risk factors. These are presented in Table 2.

Figure 1. SSC technologies

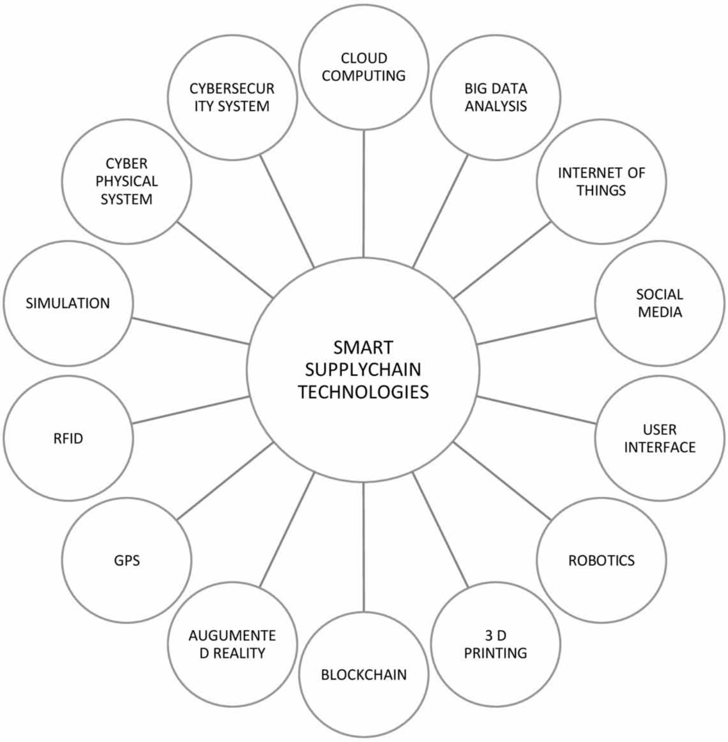


Table 1. Conclusions of the literature review

Reference	Research Objective	Research Method	Findings
Abdel-Basset et al. (2019)	Measurement of supply chain risks	Supply chain risks are quantified using the Analytic Hierarchy Process (AHP), collected through an online questionnaire and personal interviews with supply chain experts	Consistent and accurate risk values are calculated, which was impossible in the qualitative research method
Ansari et al. (2020)	Identifies and ranks solutions to mitigate supply chain risks	Literature review, survey questionnaire, and discussion with expert panels using a multi-criteria decision-making framework and fuzzy application	Provides 12 solutions to overcome the 24 supply chain risks identified
Kara et al. (2020)	Develops a data mining framework for identifying, assessing, and mitigating supply chain risks	Research-based case study validated with semi-structured interviews, discussions, and a focus group study	An SSC management framework is proposed based on data mining, which provides a complete system to collect, analyze, and manage supply chain risks
Fan & Stevenson (2018)	Reviews supply chain risk management literature, including risk identification, assessment, treatment, and monitoring; develops a conceptual framework to evaluate risks	A systematic literature review of 354 articles published between 2000 and 2016	Identified risk types and proposed mitigation strategies; ten key future research directions are identified
Aqlan (2015)	Provides an integrated framework for supply chain risk assessment	Uses a survey to identify risk factors, likelihood, and impacts to find the potential risks; values are based on experts' knowledge, historical data, and supply chain structure	Significant supply chain risks are identified

Based on the risk factors discussed in Table 2, the authors present a framework for the SSC risk assessment and then advises mitigation and monitoring strategies.

PROPOSED FRAMEWORK

After analyzing the concepts from different frameworks provided in the literature related to supply chain risk management (Aqlan, 2016; Abdel-Basset et al., 2019; Birkel et al., 2018; Fan & Stevenson, 2018; Monroe et al., 2014; Schauer et al., 2018), a new research framework is proposed and applied for SSC risk management. Figure 2 represents the framework.

Figure 2 shows a list of risk factors that were extracted by conducting a comprehensive literature review. Based on the extracted factors, a questionnaire was developed for data collection. Before data analysis, the quality of collected data in terms of reliability and validity was evaluated. A descriptive data analysis revealed the status of the implementation of smart technology in the supply chain and showed the probability of occurrence and the importance of risk factors in the supply chains studied. Then, a failure mode and effect analysis evaluated and prioritized the risk factors. Finally, a risk mitigation plan is proposed. The proposed framework can be used for risk analysis in different contexts.

METHOD

To address the research questions, the authors used quantitative and qualitative methods. A qualitative method has been employed to develop a theoretical framework for Smart Supply Chain (SSM) risk

Table 2. Risk factor descriptions and references

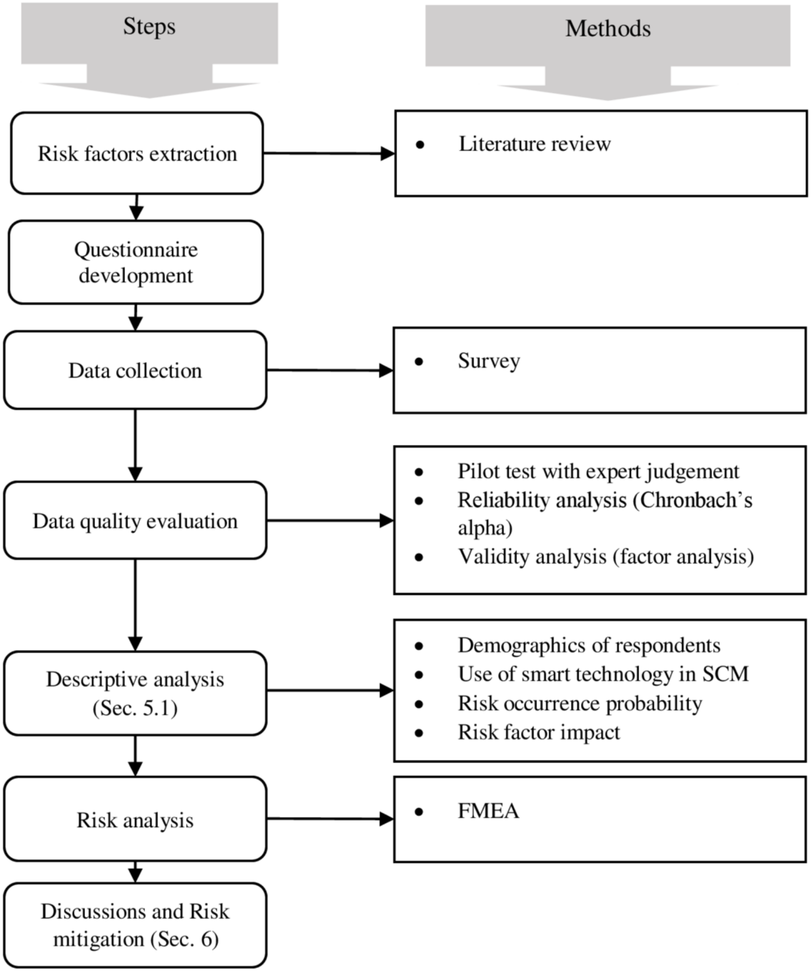
Reference	Risk Factors	Description
Amin et al. (2013)	Non-availability of IT system	In combination with the highly interconnected information network of an SSC, a non-availability of one component can spread throughout the entire network, resulting in a complete failure of the IT system.
Haschak et al. (2019)	Cyber crime	Hackers use malware to penetrate a system and breach critical data like customers' payments and personal details.
Khan & Stolte (2014)	Data breaches	The nature of SSC services is complex, relying largely on strong connectivity. If any damage happens to the connectivity, it could have serious consequences if the link carries time-sensitive supply chain scheduling data.
Gregory et al. (2016)	Lack of skilled professionals	After beginning to use smart technologies, the next biggest challenge is finding people with the right skill sets to operationalize a smart supply chain, including technical, analytical, and governance skills.
Ravulakollu et al. (2018)	Lack of communication at gateways and borders	Some ports are not equipped with smart technologies, so tracking the shipment at those destinations is very hard. Strong interconnectedness is needed across the globe.
Birkel et al. (2019)	High cost of implementation	It is assumed that implementing an SSC requires large investments with uncertain success and profitability, leading to a high implementation barrier.
Birkel et al. (2019)	System complexity	The integrated approach of the SSC—horizontal and vertical interconnection—has a lot of potential, but it is complex to implement. If complications are not resolved satisfactorily, there will be lag, and the advantages of smart technologies may not be realized.
Islam et al. (2019)	Web vulnerability	Cybercriminals could attack an organization's server that connects with a third-party financial organization network. The attacker could use SQL injection attacks to access customers' data and redirect shipments and deliveries. With some knowledge of the software composition, the adversary may cause an attack and replace legitimate software with modified versions.
Wallace (2016)	Inbound & outbound threats	Inbound and outbound supply chain risk is the potential for an adversary to disrupt the supply chain, maliciously introduce unwanted functions, or change the system's design, product, or integrity.
Riemer et al. (2019)	Lack of collaboration	Due to the complexity and costs associated with the increasingly complicated information flows, it is only possible to make full-scale applications for information sharing and collaboration in smart supply chains where information is produced and managed by machines and devices. Lacking visibility and collaboration in traditional supply chains is one of the fundamental issues smart supply chains must address.
Sundarakani et al. (2019)	Management commitment	Seamless collaboration is likely based on trust and commitment between supply chain staff and the top management. Therefore, supply chain decision-makers need to be transparent and clear in communicating with their employees to benefit from full collaboration.
Zhao et al. (2017)	Pollution	Many of the existing machines and systems will have to be replaced by smart technologies. Although attempts can be made to recycle parts of the old machines or plants and install them in the new ones, most must be dumped, ending up in landfills. This burdens the global environment, especially since the decomposition and degradation of many waste materials take a very long time.
Birkel et al. (2019)	Job loss	Smart technology could cause job losses if employees cannot quickly adapt and satisfy the new requirements. Therefore, it is to be noted that, besides the roles performed by personnel with low qualifications like repetitive tasks, planning and decision-making could also become automated, meaning that more highly qualified personnel could be in danger of job loss. Therefore, employees must be ready to develop new competencies, which might be a major risk within smart technology's social aspect.

factors. Conceptual framework has been verified and assessed using a quantitative survey research method (Ellram, 1996; Yin, 2009).

Questionnaire development

The factors were extracted from the literature, and the questionnaire is available in Appendix 1. The survey includes sections for demographics, smart technologies usage, and the probabilities and impact of risk factors. The extent of the use of smart technologies, probabilities and impact of risk factors have been measured by asking respondents to select the number that best describes their estimated values, ranging from 1 to 5 (1 Minimal, 2 Minor, 3 Moderate, 4 Significant, 5 Severe).

Figure 2. Proposed risk assessment framework


Steps
Methods
Risk factors extraction
Literature review
Questionnaire development
Data collection
Survey
Data quality evaluation
Pilot test with expert judgement
Reliability analysis (Chronbach's alpha)
Validity analysis (factor analysis)
Descriptive analysis (Sec. 5.1)
Demographics of respondents
Use of smart technology in SCM
Risk occurrence probability
Risk factor impact
Risk analysis
FMEA
Discussions and Risk mitigation (Sec. 6)

Data collection

Data (*n* = 56) were collected through a Qualtrics survey, and it took approximately 15 minutes for the respondents to complete the survey. To pilot test the study, emails were sent to four experts; they were asked to provide feedback about the questionnaire in regard to terminology and consistency with business practices and language. The questionnaire was revised based on their feedback.

Reliability test

To avoid ambiguity in questions and increase the survey data's reliability, a test of Cronbach's alpha was conducted with the 56 respondents ($\alpha = 0.864$). Cronbach's alpha ranges from zero to one, and values of 0.7 and higher are considered acceptable reliability coefficients (Nunnally & Bernstein, 1994). So, the test and the applied questions are considered reliable.

Construct validity analysis

Exploratory factor analysis (EFA) extracts the factors to determine the use and importance of the smart supply chain tools and techniques and the risk factors with their probabilities and impacts.

Table 3 shows that for smart technologies and probabilities, all questions are loaded on one factor with an eigenvalue of more than one. Then construct validity is confirmed for smart technology and probability. However, the EFA results show three latent factors with an eigenvalue of more than one, which explain 75% of the total variance for the impact construct. Three components are extracted from the factor analysis, as shown in Table 3.

The first component consists of four factors that significantly impact the supply chain processes. These include the impact of a network failure, impact of cybercrime, impact of the loss of data, and impact of web application failure. According to the Gartner Report (2021), these risk factors are included in the cybersecurity and digital risk management construct (McMillan & Proctor, 2020). According to McMillan and Proctor (2020, page:1), "The failure to manage your digital risks is likely to sabotage your digital business and expose your organization to potential impacts beyond a simple opportunity loss. The extent to which CIOs engage in digital risk management can be a crucial factor in avoiding such dangers."

The second component consists of three factors, including the impact of talent shortage, pollution and emission, and the loss of jobs. It constitutes the second construct termed corporate social responsibility (Pettey, 2017). Under this construct, organizations protect their employees from job loss, their environment from pollution, put their people first, and manage their environmental impact (Pettey, 2017).

The third component has three factors, including the impact of outbound threats, the impact of lack of collaboration, and the impact of lack of management support. In Gartner's research trends 2021, this component refers to customer service and leadership support (Omale, 2021). Management should ensure the business operation's continuity and be in regular contact with the customers to ensure their service needs are met (Omale, 2021).

RESULTS

In this section, the descriptive statistics of the participants' demographics are reported, along with descriptive statistics for the extent to which smart technologies are used, the probability of risk factors, and their impacts.

Table 3. The EFA results for impact after the occurrence of risks

Rotated Component Matrix					
The Impact of Risk Factors	**Component loading**			**Eigenvalues**	**Constructs Label**
	1	**2**	**3**		
Impact of network failure	.724			1.833	Cybersecurity and Digital Risk Management
Impact of cybercrime	.682				
Impact of loss of data	.844				
Impact of the web app. failure	.766				
Impact of talent shortage		.610		1.203	Corporate Social Responsibility
Impact of pollution & emission		.849			
Impact of loss of jobs		.773			
Impact of outbound threats			.879	1.039	Customer Service and Leadership Support
Impact of Lack of Collaboration			.824		
Impact of lack of mgt support			.853		

Descriptive statistics

Respondent demographics

In Question 1, respondents were asked about their role in the company they were working. Table 4 illustrates the distribution of the respondents' roles. Table 4 shows that most (66%) of the respondents worked as Workers in supply chain companies.

Question 2 asks about the size of the company. Table 5 elaborates on the size of the companies, showing that most (52%) employees worked in companies with more than 500 employees.

In Question 3, the respondents were asked about the industry and logistics they were involved in. Table 6 shows that most respondents worked in warehousing (21%) and manufacturing (17%).

Question 4 asks about the network size of the supply chain network and how it is spread in terms of area. Table 7 shows that 57% worked domestically and 43% worked internationally.

Table 4. Job positions of the respondents

Job designation	**Frequency**	**Percentage**	**Cumulative %**
CEO	1	1.78	1.78
Marketing Manager	2	3.57	5.35
Manager	16	28.57	33.92
Workers	37	66.08	100
Total	56		

Table 5. Size of the companies of the respondents

Size of the company	**Frequency**	**Percentage**	**Cumulative %**
Up to 100 Employees	3	5.36	5.36
100 to 500 Employees	10	17.86	23.22
More than 500	29	51.78	75
Not identified	14	25	100
Total	56	100	

Table 6. Sectors where the respondents work

Related industry	**Frequency**	**Percentage**	**Cumulative %**
Trading	3	5.36	5.36
Manufacturing	10	17.86	23.22
Software Development	6	10.71	33.93
High tech Industry	6	10.71	44.64
Transportation	9	16.07	60.71
Warehousing	12	21.43	82.14
Other	10	17.86	100
Total	56	100	

Table 7. The network size of the companies

Area	Frequency	Percentage	Cumulative%
Regional	13	23.21	23.21
Countrywide	19	33.93	57.14
Global	24	42.86	100
Total	56	100	

The extent of the use of smart technologies in smart supply chains

Question 5 asked about the technology trend in the smart supply chain. The respondents were asked about their technologies for their supply chain activities. Figure 3 shows the average trend of smart technologies in the supply chain sector. Table 8 shows the average trends and other descriptive statistics of smart technologies in the companies.

The data show that bar codes, social media, cybersecurity systems, and cloud computing are frequently used in supply chain activities.

Table 8. Extent of use of smart technologies

Trends Of Smart Technology	N	Min	Max	Mean	Std. D
Use of bar code	56	1	5	3.23	1.561
Use of social media	56	1	5	3.00	1.414
Use of cybersecurity system	56	1	5	2.79	1.385
Use of cloud computing	56	1	5	2.75	1.116
Use of robot	56	1	5	2.74	1.492
Use of IoT	56	1	5	2.63	1.287
Use of the cyber-physical system	56	1	5	2.61	1.275
Use of RFID	56	1	5	2.52	1.375
Use of simulation	56	1	5	2.45	1.292
Use of three-D	56	1	5	2.39	1.216
Use of blockchain	56	1	5	1.77	1.191
Use of augmented reality	56	1	5	1.73	1.07

Figure 3. The average trends of smart technologies in SCM

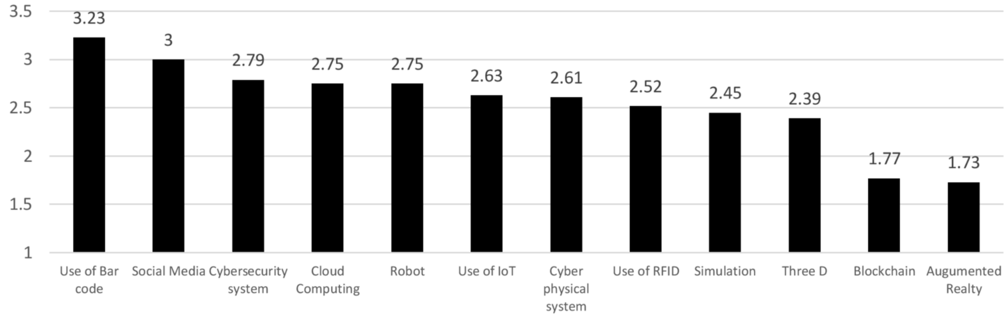


Table 9. Average probabilities of smart risk factors

Probability of Smart Risks	N	Min	Max	Mean	SD
Complexity	56	1	5	2.61	1.186
Web app. failure	56	1	5	2.45	1.278
High cost	56	1	5	2.36	1.212
Outbound threats	56	1	5	2.21	1.171
Talent shortage	56	1	5	2.16	1.108
Inbound threats	56	1	5	2.16	1.058
Pollution and emission	56	1	5	2.04	1.206
Lack of collaboration	56	1	5	2.04	1.044
Network failure	56	1	5	2	1.009
Lack of management support	56	1	4	1.95	0.883
Loss of jobs	56	1	4	1.95	0.796
Loss of data	56	1	5	1.75	0.977
Cybercrime	56	1	5	1.68	0.834

Average probability of each risk factor

The respondents were asked about the likelihood of different risks related to SSC factors in Question 6. Table 9 shows their average probabilities and standard deviations.

From Table 9, the authors concluded that the risk of complexity, web failure, and high cost for a smart supply chain are the risks with the highest probabilities. This study shows that, apart from these risk factors, human error is a common risk factor in the supply chain. Mislabeling, manual sending to other destinations, and the improper use of smart technologies are some of the examples of human error risk factor.

Average impact of the risk factors

Question 7 explains the estimated impact of the risk if it occurs in the company. These are the estimates created by experienced supply chain professionals. The average of these impacts and their standard deviations are given in Table 10.

Table 10 shows that the highest impact of an SSC's risk factors includes web failure, talent shortage, and risk of loss of data.

Risk analysis: Failure mode and effects analysis (FMEA)

A typical FMEA table for risk identification and assessment includes risk factors, frequency, severity, risk priority number, recommended risk management actions, and responsible staff (Giannakis & Papadopoulos, 2016). Table 11 presents the average of 56 samples of impacts and probabilities for each risk factor in the survey. These average impacts are multiplied by their respective probabilities to find the risk values and the final risk assessment. The average percentages and cumulative percentages are calculated in the last two columns.

Table 11 categorizes and prioritizes the risks according to their impact and likelihood. Figure 6 shows the highest risk factors, the medium-risk factors, and the low-risk factors.

Table 10. The average impact of the smart risk factors

Impact of Smart Risks	N	Min	Max	Mean	SD
Web app. failure	56	1	5	2.64	1.069
Talent shortage	56	1	5	2.61	1.039
Loss of data	56	1	5	2.57	1.11
Complexity	56	1	4	2.45	0.851
Cybercrime	56	1	4	2.39	0.888
Inbound threats	56	1	5	2.32	0.897
Pollution & emission	56	1	5	2.32	0.993
High cost	56	1	5	2.3	0.851
Outbound threats	56	1	5	2.25	0.857
Lack of collaboration	56	1	5	2.25	0.837
Network failure	56	1	5	2.23	1.191
Lack of management support	56	1	5	2.2	0.961
Loss of jobs	56	1	5	2.05	0.961

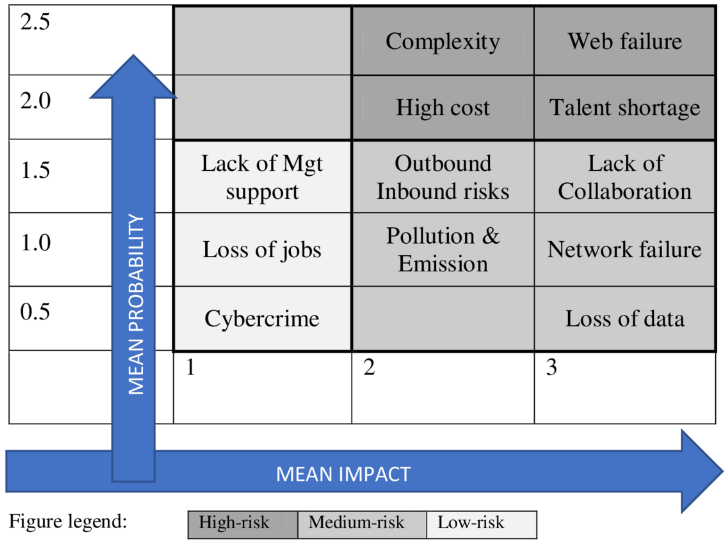
Table 11. Failure mode and effect analysis

Risk Level	Risk #	Risk Factors	Risk Code	Avg Impact	Avg Prob	Risk = Impact * Prob	% Avg	Cumulative %
Highest-risk factors	1	Risk of the web app. failure	WA	2.64	2.45	6.468	10.03	10.03
	2	Risk of complexity	RC	2.45	2.61	6.3945	9.91	19.94
	3	Risk of talent shortage	TS	2.61	2.16	5.6376	8.74	28.68
	4	Risk of the high cost	HC	2.3	2.36	5.428	8.42	37.10
Medium-risk factors	5	Risk of inbound threats	IN	2.32	2.16	5.0112	7.77	44.87
	6	Risk of outbound threats	OUTB	2.25	2.21	4.9725	7.71	52.58
	7	Risk of pollution& emission	P&E	2.32	2.04	4.7328	7.34	59.92
	8	Risk lack of Collaboration	LOC	2.25	2.04	4.59	7.12	67.03
	9	Risk of loss of data	LOD	2.57	1.75	4.4975	6.97	74.01
	10	Risk of network failure	NF	2.23	2	4.46	6.91	80.92
Low-risk factors	11	Risk of lack of mgt support	LOM	2.2	1.95	4.29	6.65	87.58
	12	Risk of cybercrime	CC	2.39	1.68	4.0152	6.23	93.81
	13	Risk of loss of jobs	LOJ	2.05	1.95	3.9975	6.19	100

CONCLUSIONS: RISK MITIGATION AND MONITORING

This paper develops a framework for smart supply chain risk factors. Different concepts are used from the literature to derive a new framework with smart technologies in the supply chain. Then, the trends of smart technologies in the supply chain system were analyzed, and their usage and importance were categorized. Risks were identified by measuring their impact and probability using a quantitative approach. Risk estimates are prioritized based on their risk values. Thus, different rankings were assigned to each risk factor according to their respective values.

Figure 4. The categorization of risk factors based on probability and their impact



2.5		Complexity	Web failure
2.0		High cost	Talent shortage
1.5	Lack of Mgt support	Outbound Inbound risks	Lack of Collaboration
1.0	Loss of jobs	Pollution & Emission	Network failure
0.5	Cybercrime		Loss of data
	1	2	3

Mitigation means minimizing risk to an acceptable level. The probability and the impact of the SSC risk factors must be evaluated. Risk mitigation strategies should be developed for risks categorized as high or medium probability (Aqlan & Lam, 2015). The selection of a risk mitigation strategy also depends on the risk type and the organization's budget (Tummala & Schoenherr, 2011). Smart supply chain organizations should carefully evaluate the acceptance, avoidance, sharing, and transfer options before selecting a mitigation strategy. As SSC risks are often interconnected, eliminating one risk type might aggravate another; hence, mitigation strategies should be employed with minimal contradiction and particular attention to those risks with negative dependences (Sarker et al., 2016).

Different smart supply chain risks may need different risk treatment strategies. Based on the limited resources, organizations will have to decide where they can be best deployed and switch to other strategies. Risk mitigation appears most suitable for high probability and low impact risks like complexity, risk of cost, and inbound threats.As Figure 4 shows, web application failure and talent shortage are the most probable risk factors with the highest impact, so investing in risk avoidance seems necessary for these risk factors. In contrast, risk acceptance may be permitted for low probability and low impact risks like loss of jobs and lack of management support (Silbermayr & Minner, 2016).

In contrast, risk transfer or sharing seems most appropriate for disruption risks with a low probability and high impacts, such as cybercrime and data loss. However, each risk's smart system will need to be continuously monitored to catch the vulnerabilities and ensure that the strategies align with the risk control. It is important to ensure that risk monitoring is based not only on judgemental assessments but also on formal processes. Staff members should monitor daily, technical support should be available 24/7, and a specific data management system for risk monitoring should be established (Tummala & Schoenherr, 2011).

While asking about the trend of smart technologies in their system, respondents replied that they use social media, bar code systems, and cloud computing most frequently. However, augmented reality, blockchain, and 3D printing are used less frequently. Blockchain, as an emerging technology, is given less importance. It is advised and strongly recommended that the companies invest in blockchain (Jabbari & Kaminsky, 2018) and 3D printing (Mohr & Khan, 2015) to achieve high efficiency and performance.

When asked about the probability of occurrence of smart risks, the maximum responses received were about the risk of complexity, web failure, and the high cost of implementation. It teaches us that a smart supply chain is not a simple system, and it bears a huge cost to be implemented. It is recommended to be fully prepared before starting a smart supply chain system to overcome the complexity (Surana et al., 2005) and cost. Controlling the complexity level can lead to higher cost efficiency and reduced risk, a win-win (Chopra & Sodhi, 2014). To get a competitive advantage, network partners must begin migrating from a cost focus to a value focus (Ross, 2002).

Asking about the impact of the smart risk, the respondents responded that web application failure, talent shortage, and data loss had been the biggest impact on the system. Therefore, it is recommended that the companies have a strong web system, fully competent and trained staff, and data security in the backup.

According to the exploratory factor analysis, cybersecurity, corporate social responsibility, customer service, and leadership support are important factors for a business system's success. It is recommended that the companies consider these aspects of the corporate culture to get a stronger ground in the economy.

The proposed framework will help managers identify the above theoretical findings for their business success. It will help practitioners better understand smart technologies' impact on their smart supply chain environment.

FUTURE RESEARCH DIRECTIONS

Future research should be done on complexity, web failure, cost, and talent shortage as the most important risk factors for the smart supply chain. This qualitative case study sheds light on the root causes of these factors. After investigating and prioritizing risk factors, we need to answer this question: How to deal with the highest risk factors? Future research should be conducted to find the reasons for poor interest in emerging technologies, including blockchain, 3D printing, and augmented reality. Despite the potential of emerging technologies, the extent of use of these technologies is not that much. Survey research on the impact of emerging technologies on supply chain performance would show companies how to unlock the potential of emerging technologies to improve supply chain performance.

REFERENCES

Abdel-Basset, M., Gunasekaran, M., Mohamed, M., & Chilamkurti, N. (2019). A framework for risk assessment, management, and evaluation: Economic tool for quantifying risks in the supply chain. *Future Generation Computer Systems*, *90*, 489–502. doi:10.1016/j.future.2018.08.035

Amin, S. H., & Zhang, G. (2013). A multi-objective facility location model for closed-loop supply chain network under uncertain demand and return. *Applied Mathematical Modelling*, *37*(6), 4165–4176. doi:10.1016/j.apm.2012.09.039

Ansari, Z. N., Kant, R., & Shankar, R. (2020). Evaluating and ranking solutions to mitigate sustainable remanufacturing supply chain risks: A hybrid fuzzy SWARA-fuzzy COPRAS framework approach. *International Journal of Sustainable Engineering*, *13*(6), 473–494. doi:10.1080/19397038.2020.1758973

Aqlan, F. (2016). A software application for rapid risk assessment in integrated supply chains. *Expert Systems with Applications*, *43*, 109–116. doi:10.1016/j.eswa.2015.08.028

Aqlan, F., & Lam, S. S. (2015). Supply chain risk modeling and mitigation. *International Journal of Production Research*, *53*(18), 5640–5656. doi:10.1080/00207543.2015.1047975

Birkel, H. S., & Hartmann, E. (2019). Impact of IoT challenges and risks for SCM. *Supply Chain Management*, *24*(1), 39–61. doi:10.1108/SCM-03-2018-0142

Chopra, S., & Sodhi, M. (2014). Reducing the risk of supply chain disruptions. *MIT Sloan Management Review*, *55*(3), 72–80.

Ellram, L. M. (1996). The use of the case study method in logistics research. *Journal of Business Logistics*, *17*(2), 93.

Fan, M., & Sharma, A. (2021). Design and implementation of construction cost prediction model based on SVM and LSSVM in industries 4.0. *International Journal of Intelligent Computing and Cybernetics*.

Fan, Y., & Stevenson, M. (2018). A review of supply chain risk management: Definition, theory, and research agenda. *International Journal of Physical Distribution & Logistics Management*, *48*(3), 205–230. doi:10.1108/IJPDLM-01-2017-0043

Gartner Inc. (2021). *Gartner top security projects for 2020-2021*. Gartner. Retrieved April 5, 2022, from https://www.gartner.com/smarterwithgartner/gartner-top-security-projects-for-2020-2021

Giannakis, M., & Papadopoulos, T. (2016). Supply chain sustainability: A risk management approach. *International Journal of Production Economics*, *171*, 455–470. doi:10.1016/j.ijpe.2015.06.032

Hofmann, E., & Rüsch, M. (2017). Industry 4.0 and the current status as well as future prospects on logistics. *Computers in Industry*, *89*, 23–34. doi:10.1016/j.compind.2017.04.002

Jabbari, A., & Kaminsky, P. (2018). *Blockchain and supply chain management*. Department of Industrial Engineering and Operations Research University of California.

Kara, M. E., Fırat, S. Ü. O., & Ghadge, A. (2020). A data mining-based framework for supply chain risk management. *Computers & Industrial Engineering*, *139*, 105570. doi:10.1016/j.cie.2018.12.017

Lee, J., Bagheri, B., & Kao, H.-A. (2015). A cyber-physical systems architecture for industry. *Manufacturing Letters*, *4*, 18–23. doi:10.1016/j.mfglet.2014.12.001

McMillan, R., & Proctor, P. (2020). *Cybersecurity and risk management*. Gartner. https://www.gartner.com/en/doc/3846477-cybersecurity-and-digital-risk-management-cios-must-engage-and-prepare

Mohr, S., & Khan, O. (2015). 3D printing and its disruptive impacts on supply chains of the future. *Technology Innovation Management Review*, *5*(11), 20–25. doi:10.22215/timreview/942

Monroe, R. W., Teets, J. M., & Martin, P. R. (2014). Supply chain risk management: An analysis of sources of risk and mitigation strategies. *International Journal of Applied Management Science*, *6*(1), 4–21. doi:10.1504/IJAMS.2014.059291

Nunnally, J. C., & Berstein, I. H. (1994). The assessment of reliability. *Psychometric Theory*, *3*, 248–292.

Omale, G. (2021). *Top customer service and support predictions for 2021 and beyond*. Gartner. https://www.gartner.com/smarterwithgartner/top-customer-service-and-support-predictions-for-2021-and-beyond

Pettey, C. (2017). *Leading supply chains in a disruptive world*. Gartner. https://www.gartner.com/smarterwithgartner/leading-supply-chains-in-a-disruptive-world/

Porter, M. E., & Heppelmann, J. E. (2014). How smart, connected products are transforming competition. *Harvard Business Review*. https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition

Ravulakollu, A. K., Urciuoli, L., Rukanova, B., Tan, Y. H., & Hakvoort, R. A. (2018). Risk-based framework for assessing resilience in a complex multi-actor supply chain domain. *Supply Chain Forum: An International Journal, 19*(4), 266–281.

Riemer, K., Schellhammer, S., & Meinert, M. (2019). *Collaboration in the digital age. How technology enables individuals, teams, and businesses*. Springer. doi:10.1007/978-3-319-94487-6

Ross, D. F. (2002). *Introduction to e-supply chain management: Engaging technology to build market winning business partnerships*. CRC Press. doi:10.1201/9781420025415

Schlüter, F., & Henke, M. (2017). Smart supply chain risk management: A conceptual framework. *Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment. Proceedings of the Hamburg International Conference of Logistics (HICL)*, *23*, 361–380.

Schwab, K. (2019). *The global competitiveness report*. World Economic Forum. https://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf

Sharma, A., & Kumar, N. (2021). Third eye: An intelligent and secure route planning scheme for critical services provisions on the internet of vehicles environment. *IEEE Systems Journal*, *16*(1), 1217–1227. doi:10.1109/JSYST.2021.3052072

Shelton, T. (2013). PwC Thought leadership on social, mobile, analytics, cloud (SMAC). In Business models for the social, mobile cloud: Transform your business using social media, mobile internet, and cloud computing (pp. 165–216). Wiley.

Silbermayr, L., & Minner, S. (2016). Dual sourcing under disruption risk and cost improvement through learning. *European Journal of Operational Research*, *250*(1), 226–238. doi:10.1016/j.ejor.2015.09.017

Sun, H., Fan, M., & Sharma, A. (2021). *Design and implementation of construction prediction and management platform based on building information modeling and three-dimensional simulation technology in industry 4.0*. IET Collaborative Intelligent Manufacturing.

Sundarakani, B., Kamran, R., Maheshwari, P., & Jain, V. (2019). Designing a hybrid cloud for a supply chain network of industry 4.0: A theoretical framework. *Benchmarking*.

Surana, A., Kumara, S., Greaves, M., & Raghavan, U. N. (2005). Supply-chain networks: A complex adaptive systems perspective. *International Journal of Production Research*, *43*(20), 4235–4265. doi:10.1080/00207540500142274

Xu, L. D., Xu, E. L., & Li, L. (2018). Industry 4.0: State of the art and future trends. *International Journal of Production Research*, *56*(8), 2941–2962. doi:10.1080/00207543.2018.1444806

Yin, R. K. (2009). How to do better case studies. The SAGE handbook of applied social research methods, 2, 254–282.

APPENDIX 1

Survey Questionnaire

Q1. What best describes your role in your company?
Q2. What best describes the size of your company?
Q3. Your business belongs to which industry?
Q4. Is your supply chain network local, regional, or international?
Q5. Please indicate the extent to which your company's supply chain system has used the following technologies by marking the alternative that best describes your idea, ranging from 1 to 5: (1 not at all, 3 to some extent, 5 strongly).

Smart Technologies

- Robotics
- Sensors – IoT
- Blockchain
- 3D Printing
- Augmented Reality
- Simulation
- Cyber-Physical System
- Cybersecurity System
- Cloud Computing
- RFID
- Barcode
- Social Media
- Other

Q6. On a scale from 1 (not at all) to 3 (to some extent) to 5 (extremely high), how frequently do the following risks happen in your organization?

- Risk Factors
- Network Failure
- Cybercrime
- Loss of Data
- Talent shortage
- Web Application
- Pollution & Emission
- The high cost of implementation
- Risk of complexity
- Inbound threats
- Outbound threats
- Lack of Collaboration
- Lack of management support
- Job losses
- Other

Q7. Please rate the impact you evaluate in your organization after the mentioned risks by marking the alternative that best describes your idea, ranging from 1 to 5: (1 Minimal, 2 Minor, 3 Moderate, 4 Significant, 5 Severe).
Q8. Please provide any other probable comments or advice you may have about smart tech in the supply chain, probability, and the importance of risk factors.

Khalid Khan is a graduate of Management Sciences from the TED Rogers School of Management at Toronto Metropolitan University.. He has academic experience of more than 15 years. He taught Management and business studies in different colleges of Great Toronto. Right now, he is working as a lecturer of management studies in a public college in Ontario, Canada.

Abbas Keramati is an assistant professor of teaching at the State University of New York at Buffalo.. He has been teaching in the University of Toronto and Toronto Metropolitan University. He was Associate Professor of the School of Industrial Engineering at University of Tehran. Dr. Keramati was also Assistant Professor of Information Technology Management at the Toronto Metropolitan.