Dutch Journal of Finance and Management
2022, 5(2), 22405
e-ISSN: 2542-4750
https://www.djfm-journal.com/

Research Article

OPEN ACCESS

Managing Supply Chain Risk with the Integration of Internet of things in the manufacturing Sector of Pakistan

Prince Kumar [1 2 *], Shahid Aziz [3]

[1] Shaheed Zulfikar Ali Bhutto Institute of Science and Technology, Karachi, Pakistan
[2] Institute of Business Management Karachi, Karachi, Pakistan
[3] Asia e University, Selangor, Malaysia
* **Corresponding Author:** prince.rajput06@gmail.com

Citation: Kumar, P., and Aziz, S. (2022). Managing Supply Chain Risk with the Integration of Internet of things in the manufacturing Sector of Pakistan. *Dutch Journal of Finance and Management*, 5(2), 22405. https://doi.org/10.55267/djfm/13676

ARTICLE INFO

ABSTRACT

In the ever-evolving landscape of global trade and manufacturing, supply chain resilience has emerged as a vital concern for organizations operating in the manufacturing sector. This research study delves into the critical domain of managing supply chain risk through the integration of Internet of Things (IoT) technologies within the manufacturing sector of Pakistan. With the advent of Internet of Things, the manufacturing industry in Pakistan has witnessed transformative opportunities to enhance operational efficiency and mitigate supply chain vulnerabilities. This qualitative study engaged ten seasoned supply chain professionals through in-depth interviews to discern the multifaceted impact of IoT integration on risk management within the manufacturing sector. The results of this study, analyzed using thematic analysis within Nvivo software, illuminate the implications of using the Internet of Things in supply chain risk management, the aim is to understand how the Internet of things influences and impacts the supply chain risk management process, both internally and externally, and the resulting outcomes. The study is guided by the information processing theory and employs a methodology based on theory to investigate the information requirements and processing capabilities of supply chain risk management supported by the internet of things. The findings of the study reveal that the organizations involved experienced increased data availability, which led to improved process transparency and management. Supply chain risk management also showed enhancements across its various stages, including risk transparency, risk awareness, and risk strategies. These improvements provided a competitive advantage by aligning the information needs with the information processing capabilities. The study provides detailed insights into the structure of internet of things systems, main use cases, and the impact on the supply chain risk management process, offering valuable information for managers. It highlights the benefits of increased data availability, improved process transparency, and management, as well as the implications for personnel and potential barriers. The findings provide valuable insights for Supply chain managers and pave the way for further research in this area.

Keywords: Supply chain, Internet of things, Risk Management, Technology, Supply chain risk management, Information processing theory

INTRODUCTION

In today's increasingly interconnected and dynamic business landscape, the effective management of supply chain risks has become a critical priority for organizations across industries (Tsang et al., 2018). The advent of the Internet of Things (IoT) has ushered in a new era of possibilities, reshaping traditional supply chain processes and offering transformative opportunities for mitigating risks (Kieras, Farooq and Zhu, 2021). This research paper aims to explore

and analyze the profound impact of IoT on Supply Chain Risk Management (SCRM) and its implications for organizational resilience and competitiveness (Birkel and Hartmann, 2020). The IoT represents a network of interconnected physical devices embedded with sensors, software, and communication capabilities, enabling them to collect and exchange data autonomously. By seamlessly integrating the physical and digital realms, IoT devices offer unprecedented visibility and insights into various aspects of the supply chain, from raw material sourcing to product delivery (Harsasi and Minrohayati, 2017). This enhanced visibility empowers organizations with real-time information, enabling them to identify, assess, and respond to potential risks proactively. One of the key advantages of IoT in SCRM lies in its ability to provide granular and real-time data on supply chain operations. Through the deployment of IoT sensors and devices, organizations can collect a wealth of data points, such as temperature, humidity, location, and condition of goods, at different stages of the supply chain (Kothari, Jain and Venkteshwar, 2018). This real-time data enables organizations to monitor and track their assets, detect anomalies, and identify potential risks and disruptions swiftly. Consequently, organizations can take timely corrective actions, minimizing the impact of disruptions and enhancing their overall risk mitigation strategies (Manuj and Mentzer, 2008). This research paper will delve into the various dimensions of this transformative impact, providing valuable insights and practical recommendations for organizations navigating the IoT-driven SCRM landscape. The paper is structured as follows. First, we establish the foundational knowledge by conducting a thorough literature review on supply chain management, the challenges posed by supply chain risks, and the applications of IoT in this context. We then elucidate the methodology employed in our research, including data collection methods and analytical approaches. Subsequently, we delve into the specific landscape of IoT integration and discuss the existing challenges and opportunities. Following this, we explore the ways in which IoT can be leveraged to enhance supply chain risk management, supported by real-world examples and case studies. In the results section, we present the findings of our qualitative study and, in the discussion section, interpret these findings in light of existing research. Finally, we conclude with a summary of key insights, implications for practice, and suggestions for future research directions. Through this structured approach, we aim to provide a comprehensive understanding of how IoT can be a transformative tool in bolstering supply chain resilience within Pakistan's dynamic manufacturing landscape.

LITERATURE REVIEW

Supply chain risks management

In the realm of risk literature, there is a common practice of categorizing risks as either quantifiable or objective, which is crucial in the business environment (Ho, 2015). Supply chain risk management (SCRM) employs quantitative evaluation methods to provide numerical estimates of risks based on their likelihood of occurrence and impact (Christopher, 2004). However, due to the complexity of modern supply networks, comprehending all potential risks becomes challenging as multiple risks can emerge. Furthermore, the unique network architecture within a supply chain's business ecosystem significantly influences risk profiles and interdependencies (Varzandeh, 2016). To enhance transparency and facilitate informed decision-making, businesses are increasingly required to share a wide range of risk-related data. This growing need for data accessibility highlights the importance of both data availability and the ability to achieve high process efficiency (Fan, 2016).Supply chain risk management (SCRM) differs from traditional risk management approaches by adopting a cross-company perspective to identify and manage risks across the entire supply chain (Wiengarten, 2016). It recognizes that any disruptions within the supply chain should be addressed with a collaborative mindset, focusing on building effective processing capabilities to minimize vulnerability and ensure business continuity. This collaborative approach is crucial, as SCRM aims not only to reduce costs and vulnerabilities but also to ensure long-term profitability and growth. In line with (Hiromoto, Haney and Vakanski, 2017) definition, this study considers the comprehensive nature of SCRM, which encompasses both the internal and external pathways and aligns with the overall goals of the SCRM process. Supply chain risk management involves the identification, assessment, treatment, and monitoring of risks within the supply chain. According to (Harsasi and Minrohayati, 2017) the internal implementation of various tools, techniques, and strategies, as well as external coordination and collaboration with supply chain members. The ultimate goal is to reduce vulnerability and ensure the continuity and profitability of the supply chain, thereby gaining a competitive advantage.

Supply Chain Risk

Risk Identification

This step involves identifying potential risks and disruptions within the supply chain. It includes both internal risks within the organization and external risks arising from the broader business environment. Risk identification serves as the initial step in the SCRM process. Its primary objective is to uncover all pertinent risks within the supply chain and their sources. This step aims to increase visibility and reveal potential future uncertainties, enabling proactive risk management(Al-Ayed and Al-Tit, 2023). It is crucial because countermeasures can only be implemented if risks are identified (Tsang et al., 2018). Additionally, inadequate visibility and delayed information severely impact the ability to make accurate evaluations and decisions, even for risks that have already been identified (Tchankova, 2002). By conducting a thorough risk identification process, organizations can enhance their understanding of the potential risks that may impact their supply chain. This includes identifying risks related to suppliers, transportation, demand fluctuations, natural disasters, geopolitical factors, and other variables that may pose threats (Kieras, Farooq and Zhu, 2021). The goal is to improve the visibility of risks and uncertainties, enabling organizations to take proactive measures to mitigate or manage those risks effectively. Through effective risk identification, organizations can enhance their preparedness and develop appropriate risk management strategies.

Risk Assessment

Once the risks are identified, a thorough assessment is conducted to understand their potential impact and likelihood of occurrence. This evaluation helps prioritize risks based on their severity and enables the allocation of appropriate resources for mitigation. The second step in the SCRM process involves identifying the potential impact of each identified risk on the overall performance of the supply chain (Aven, 2016). Quantitative evaluation techniques are utilized to prioritize risks and provide a foundation for selecting appropriate treatment approaches (Noor, Khalfan and Maqsood, 2013). However, this step poses challenges as it needs to be thorough, efficient, and cost-effective simultaneously. Literature recommends employing a standardized process that incorporates both formal and informal components to achieve these objectives (Eisenhardt et al., 2020). However, it is challenging to generalize treatment types since each risk instance needs to be assessed individually, adding to the complexity of SCRM. Each risk instance requires careful examination and consideration to determine the most appropriate treatment strategy. The complexity of SCRM arises from the need to tailor the treatment approach to the specific characteristics and context of each risk scenario. By adopting a systematic approach to risk treatment, organizations can effectively manage and mitigate risks, improving the overall performance and resilience of their supply chain. Risk treatment can be further categorized as proactive or reactive(Hiromoto, Haney and Vakanski, 2017). Proactive strategies involve taking actions to reduce risks before they occur. These methods, such as contractual agreements, increased visibility, or supplier development, aim to decrease the likelihood or impact of potential disruptive events in advance. Risk monitoring is an integral part of the SCRM process and involves continuously assessing identified risks and evaluating the effectiveness of existing risk mitigation measures. This step allows for the identification of any changes or emerging risks, enabling organizations to adapt their strategies accordingly.

Risk Treatment

In this step, strategies and measures are implemented to treat or mitigate the identified risks. This can include preventive measures, contingency plans, risk transfer through insurance, or collaborating with supply chain partners to develop joint risk management approaches (Eisenhardt et al., 2020).

Risk Monitoring

Continuous monitoring of the identified risks is crucial to ensure their effectiveness and detect any emerging risks. This involves collecting real-time data, utilizing risk monitoring tools and technologies, and maintaining communication channels with relevant stakeholders. Risk monitoring activities may include ongoing analysis, tracking of key performance indicators, and realigning risk mitigation measures as necessary (Tsang et al., 2018). Despite its importance, risk monitoring is often overlooked in both theory and practice. However, it plays a crucial role in ensuring the effectiveness and relevance of risk management efforts. By regularly monitoring and reassessing risks, organizations can stay vigilant and proactive in addressing potential disruptions, improving their overall resilience and adaptability (Kieras, Farooq and Zhu, 2021). A systematic approach is recommended for risk monitoring, similar to the other steps in

the SCRM process. This involves establishing clear processes and guidelines for on-going risk assessment, analysis, and decision-making to ensure that risk monitoring activities are conducted effectively and consistently (Kieras, Farooq and Zhu, 2021).

Internal Route: This refers to the internal activities and processes within an organization to manage supply chain risks. It involves coordination among different departments, information sharing, and decision-making to implement risk management strategies effectively (Kotzab et al., 2015).

External Route: The external route represents the collaboration and coordination with external stakeholders, including suppliers, customers, logistics providers, and regulatory bodies. This entails sharing relevant risk information, establishing communication channels, and jointly managing supply chain risks. The conceptual framework illustrates how supply chain disruptions are processed through the individual steps of the SCRM process, while considering both the internal and external routes (Birkel and Hartmann, 2020). It provides a visual representation of the flow of activities, information, and collaboration involved in managing supply chain risks, ultimately leading to the desired SCRM outcomes.

Internet of Things

The "Internet of Things" (IoT) refers to a concept introduced by Kevin Ashton in 1999. It involves connecting computer systems embedded in physical objects to enable them to collect and store data autonomously, without the need for direct human intervention (Kothari, Jain and Venkteshwar, 2018). The IoT encompasses a network of interconnected devices, sensors, and systems that communicate and interact with each other over the internet. In the context of SCRM, the IoT plays a significant role in enhancing the collection, transmission, and analysis of data related to supply chain risks (Kayis, Erhun and Plambeck, 2013). Through the integration of IoT devices and sensors within the supply chain, real-time information can be gathered from various points, providing visibility and transparency into the status and performance of critical assets, processes, and environmental conditions. The IoT enables the seamless exchange of data among supply chain stakeholders, facilitating improved coordination, collaboration, and decision-making. It allows for the automation of data capture and analysis, leading to enhanced accuracy, efficiency, and timeliness in risk identification, assessment, and monitoring. With the IoT, supply chain managers and practitioners can access a wealth of data that was previously unavailable or difficult to obtain. This data can be utilized to gain insights into potential risks, predict disruptions, and implement proactive measures to mitigate or prevent them. The IoT also enables the implementation of real-time monitoring and tracking systems, allowing for rapid response and timely risk management actions. The "Internet of Things" (IoT) can be defined as a network of physical objects that are digitally connected to sense, monitor, and interact within a company and across its supply chain. This interconnected network enables various benefits such as agility, visibility, tracking, and information sharing, which in turn facilitate timely planning, control, and coordination of supply chain processes. By leveraging IoT technologies, companies can connect their physical assets, devices, and systems, allowing them to collect and transmit real-time data. This data can encompass a wide range of information, including inventory levels, product conditions, equipment performance, environmental factors, and customer demand patterns. With IoT-enabled sensors and devices embedded in objects throughout the supply chain, companies can gain better visibility into the status and location of goods, monitor their condition during transportation or storage, and track their movements in real time. This visibility enhances decision-making capabilities, enabling proactive risk management and efficient response to disruptions. It also enables the integration of supply chain planning and execution systems, enabling seamless communication and coordination between different stages of the supply chain. The Internet of Things (IoT) has evolved to encompass a wide range of technologies beyond just RFID. It now includes technologies such as near-field communication (NFC), wireless sensors, actuators, and smart objects (Atzori, 2010). This expanded integration of technologies allows for a diverse set of devices and systems to be interconnected within the IoT ecosystem. One of the key advantages of IoT systems is their scalability. New sensors or external data sources can be easily integrated into the existing IoT infrastructure, allowing for the continuous growth and expansion of data collection capabilities (Xu, 2014). IoT technologies enable the collection of data on a large scale, from a variety of sources, and at a high speed. In the context of SCRM, IoT-enabled devices and sensors can capture detailed information about the location, temperature, shock, and other variables related to supply chain processes. This information enhances data interchange, agility, and visibility, allowing organizations to make informed decisions and take timely actions to manage risks.

Information processing theory in the context of supply chain risk management

The information processing theory (IPT) is employed as a theoretical framework to understand the impact of IoT on SCRM. IPT has gained significant acceptance in various domains, such as information systems and decision science(Fan

et al., 2017). This theoretical perspective views firms as information processing systems that deal with uncertainty and disturbances. It recognizes that organizational activities revolve around gathering, interpreting, synthesizing, and coordinating information in the context of decision-making (Kieras, Farooq and Zhu, 2021). According to IPT, the efficient and effective processing and interpretation of information are crucial for success, rather than simply reacting to stimuli. When an organization operates as an information processing system, coordinating structures, processes, and information technologies (IT) ensure that information processing requirements align with the available processing capabilities (Aven et al., 2020). This alignment between information needs and processing capabilities enhances the efficiency and effectiveness of activities within the organization. In the context of SCRM and IoT, IPT provides insights into how organizations can leverage IoT technologies to improve their information processing capabilities. The integration of IoT in SCRM enables the collection, analysis, and dissemination of real-time data across the supply chain, facilitating better risk assessment and decision-making. By aligning information requirements with the capabilities provided by IoT, organizations can enhance their SCRM processes and ultimately achieve competitive advantages. By employing IPT as a theoretical framework, this study aims to shed light on how the information requirements and processing capabilities of SCRM are supported by IoT. It explores how the use of IoT technologies enhances data availability, process transparency, and risk management in SCRM. Additionally, the study addresses implications for personnel, incentives, and barriers, which can contribute to rethinking SCRM practices in the context of IoT. The information processing theory (IPT) is employed as a theoretical framework to understand the impact of IoT on SCRM. IPT has gained significant acceptance in various domains, such as information systems and decision science (Fan et al., 2017). When an organization operates as an information processing system, coordinating structures, processes, and information technologies (IT) ensure that information processing requirements align with the available processing capabilities (Kieras, Farooq and Zhu, 2021). This alignment between information needs and processing capabilities enhances the efficiency and effectiveness of activities within the organization.

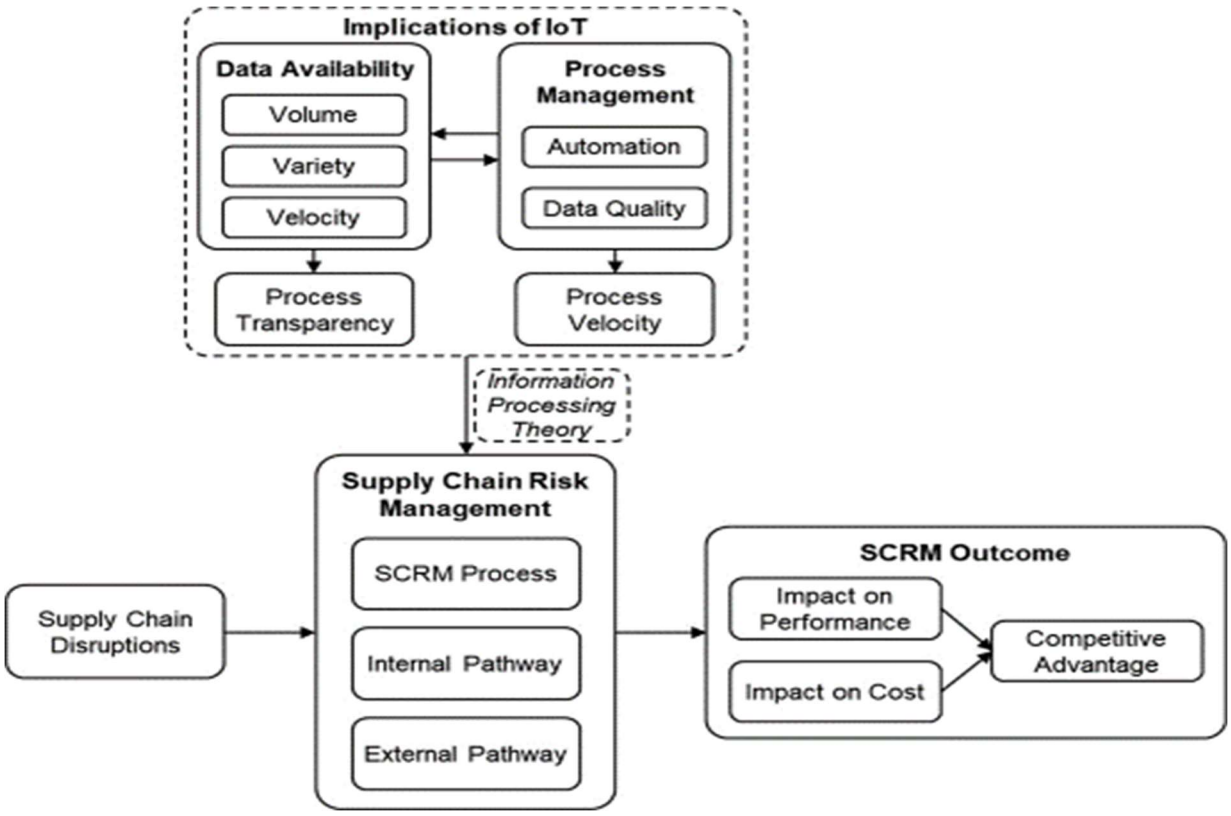

Figure 1. Conceptual framework

METHODOLOGY

Research design

To gain a comprehensive understanding of the impact of IoT on supply chain risk management (SCRM), a multi-case study approach was adopted in this research. This approach was chosen due to several reasons. Firstly, a case study allows for an in-depth investigation of a contemporary phenomenon within its real-world context, providing valuable insights into the complex nature of IoT in SCRM. The interactive features of IoT and its multifaceted influence on various elements make it suitable for a case study approach. Secondly, the objective of this research was to examine how IoT is utilized across different enterprises and its specific impact on the SCRM process. By studying multiple cases, a broader perspective can be obtained, enabling a more comprehensive analysis of IoT's role in SCRM. Furthermore, the multiple case strategy enhances the validity and generalizability of the research findings compared to a single case study. It allows for the identification of common patterns, differences, and emerging themes across different cases, thereby strengthening the grounded nature of the research. To analyze the data collected from the cases, a grounded theory approach was employed. This approach involves systematically organizing and exploring raw empirical data to develop a theoretical framework that is firmly grounded in the data. It ensures that the findings are derived from the observed phenomena and enables the development of a robust theoretical understanding of the impact of IoT on SCRM. Overall, the multi-case study approach, combined with the grounded theory methodology, This study adopts a qualitative approach, wherein interviews were carried out with ten supply chain professionals from Pakistan's manufacturing sector. The findings were analyzed using thematic analysis within the NVivo software, provides a rigorous and comprehensive approach to investigating the utilization of IoT in SCRM and its implications for businesses.

Research Question

To find out the impact of IoT, considering the Information Processing Theory (IPT) and its influence on the process, internal and external pathways, and outcomes of SCRM?

Sampling

The selection of cases for the study was guided by the aim of achieving a representative sample and ensuring comparability among the cases. The following criteria were used to select the cases:

Table 1. Sample selecting Criteria

Criteria for Sampling	Detail
Industry Focus	The target audience for the study was confined to companies in the manufacturing industry. This sector was chosen because it deals with supply chains involving tangible items, making SCRM particularly relevant.
Geographic Location	The manufacturing and selling operations of all participating companies had to be primarily situated in Pakistan. This criterion ensured that the selected companies operated under similar infrastructural, legal, and political conditions, enhancing comparability.
Adoption of IoT Technology	Companies were required to demonstrate their digital skills by adopting IoT technology in their supply chain activities. This criterion ensured that the selected cases provided insights into the utilization of IoT in SCRM.
International Operations and Intermodal Supply Chains	The companies included in the study needed to have internationally run operations with intermodal and globally connected supply chains. This criterion allowed for the exploration of the full potential of IoT in SCRM across different geographical regions and supply chain configurations.
Business-to-Business (B2B) and Business-to-Consumer (B2C) Environments	Both end-product manufacturers and suppliers operating in the B2B and B2C environments were included in the study. This criterion ensured the inclusion of a diverse range of companies with different customer-facing and supply chain dynamics.

Data collection

During the data collection process, the researchers utilized multiple sources of evidence, with interviews being the primary data source. The interviews were conducted with department leaders and subject matter experts in supply chain management (SCM), procurement, and production planning. These individuals were selected for their expertise and knowledge in the field.

Before conducting the formal research interviews, two preliminary interviews were conducted with industry experts to clarify any ambiguities or misconceptions in the questionnaire. These preliminary interviews helped refine the interview questions and ensure their effectiveness. A total of 18 interviews were conducted between mid-2022 and the beginning of 2023. The interviews were conducted over the phone and had an average duration of 25 to 30 minutes. During the interviews, detailed notes were taken independently by the researchers, and these notes were later discussed and synthesized. To enhance the validity of the information and avoid misconceptions and ambiguities, each participant was provided with a copy of the transcript to review and validate the accuracy of their responses.

Table 2. Profile of Interview companies

Case Number	Designation of Contact Person	Sector	Type of Business
1	Supply Chain Manager	Automobile	B2C
2	Product Manager	Textile	B2B & B2C
3	GM Supply Chain	Automobile Supply	B2B & B2C
4	Head of logistics	Electronics	B2C
5	Supply Chain Executive	Medical	B2B & B2C
6	Manager Procurement	Textile	B2B & B2C
7	GM Logistics	Textile	B2C
8	AM Distribution	Consumer Goods	B2C
9	Planning Officer	Technology	B2C
10	Logistic Executive	Textile	B2C

Data analysis

In the data analysis process, the researchers applied open coding, following the approach developed by Corbin and Strauss (1990). The unstructured material from each interview was analyzed using open coding to cluster and connect relevant information, uncover significant categories, and identify structures and correlations. The analysis was conducted iteratively, with researchers reviewing verified transcripts, identifying relevant material, and assigning them to categories. The coding process involved creating thematic and level-based categories by paraphrasing relevant statements and organizing them into subcategories. Initially, fact codes were used to objectively evaluate and define the substance of the statements. These fact codes were then transformed into thematic codes to categorize and group the results. This process was carried out for each interview, gradually refining and modifying the categories. To reduce bias and validate the findings, secondary data were incorporated into the analysis. By using the same categories across all transcripts, the researchers were able to compare the interviews from different businesses effectively, ensuring consistency.

To facilitate the management of large volumes of data and support the iterative coding and categorization process, a computer-aided qualitative data analysis program was utilized. This software assisted in organizing and classifying the data.

Table 3. Interview Responses Summary

IOT Impact on	Explanation	Quotes from interview
Risk Identification	Risk identification is the process of systematically identifying, recognizing, and understanding potential risks that could affect an organization, project, or system (Tchankova, 2002).	IoT technologies provide a wealth of real-time data and insights that can greatly enhance the identification and understanding of risks. The experts from manufacturing highlights the IoT influences risk identification as Real-time Data Collection, Granular Visibility, Data Analytics and Pattern Recognition, Predictive Analytics.
Risk Assessment	Risk assessment is the evaluating and analyzing identified risks to determine their likelihood of occurrence and potential impact on objectives, typically involves quantifying or qualifying risks (Aven, 2016)	IoT technologies offer real-time information and valuable insights that significantly improve the precision and efficiency of risk assessment procedures. Most of the interviewee says that the crucial ways in which IoT impacts risk assessment: immediate data collection, enhanced data accuracy, amplified data volume, improved visibility, predictive analytics, and real-time monitoring with alerts.
Risk Treatment	selecting and implementing strategies and actions to manage, mitigate, transfer, or accept risks identified through risk assessment, And measures to reduce the likelihood of risk occurrence, minimize the potential impact of risks (Purdy, 2010)	Risk mitigation is given the highest priority among the various strategies for managing risks. This is not surprising since IoT offers the capability to make fast and well-informed decisions by leveraging real-time data, thereby preventing disruptions and minimizing the impact of events.
Risk Monitoring	Provides organizations with real-time insights into their risk landscape, allowing them to take proactive actions to mitigate or respond to risks appropriately(Bedard et al., 2008).	According to industry experts, risks are dynamic and necessitate ongoing monitoring, which should be facilitated by formal processes and subjective evaluations
Internal Pathway	Refers to the flow of goods, information, and processes within an organization's internal operations to support the effective and efficient management of the supply chain (Kotzab et al., 2015)	The application of IoT in Internal pathway of supply chain management promotes higher risk transparency, improved risk knowledge, and enhanced risk strategies. This is facilitated by increasing data availability and enhanced risk process management. Here are the key ways in which IoT contributes to these benefits: Data Availability, Real-time Risk Monitoring, Predictive Analytics, and Enhanced Risk Process Management
External Pathway	Provide the structure for the flow of goods, information, and processes between the organization and external entities such as suppliers, customers, distributors, and other partners in the supply chain network (Gold and Schleper, 2017).	IoT can enhance supplier selection processes by providing more comprehensive and accurate information. IoT facilitates the flexibility of sourcing strategies.They can identify alternative suppliers, optimize transportation routes, or adjust sourcing strategies based on the data gathered from IoT devices.
Supply Chain Risk Management Outcome	The outcome of effective supply chain risk management is to minimize the impact of risks on the organization's supply chain operations and ensure the continuity of supply. By implementing robust risk management practices, organizations can achieve several positive outcomes (Birkel and Hartmann, 2020)	Indeed, the application of IoT in SCM can lead to improved SCRM performance and overall cost reductions, which can potentially result in a competitive advantage for organizations. Here are some key reasons which interviewee mentioned why IoT implementation can have such benefits: Enhance Risk Visibility, Timely Risk mitigation, proactive maintenance and quality control, optimization of inventory and logistic and finally the data driven decision making.

ANALYSIS

Structure of Internet of Things systems

An overview of the structure of IoT systems, which is relevant for analysing how SCRM (Supply Chain Relationship Management) is influenced by IoT implementation. The importance of different tiers within IoT systems and the types of sensors and technologies used in each tier. At the sensing layer, wirelessly interconnected sensors and global

positioning systems (GPS) are mentioned, including technologies like RFID (Radio Frequency Identification) and GPS. While RFID is commonly used in various applications, the specific types of sensors employed in these applications can vary. Temperature, air pressure, and vibration sensors are frequently utilized, but there are also cases where optical and humidity sensors are used. The service and interface layer encompass both internal and external services and applications. The passage mentions that seven out of twelve organizations developed their software in-house, while the remaining four organizations augmented their internal development with external expertise. This indicates that there is a mix of internally developed and externally sourced software in IoT systems. Data inputs at the service layer can be both internal and external. Internal data inputs may include supplier rankings, communications, and self-identified risks, while external data inputs can come in the form of messages or machine data from suppliers.

Impact of the Internet of Things on supply chain risk management

The research framework in this case study is designed to provide practical insights into the structure of IoT systems and their implications for supply chain risk management (SCRM). It is built upon a theoretical foundation to guide the research activities and answer the research question. By conducting a case study, the researchers were able to gather empirical data and gain a deep understanding of the IoT systems implemented in various organizations. The outcomes of the case study provide valuable context and real-world examples that support the discussion of the framework's components and consequences. The framework incorporates theoretical concepts and principles from relevant literature, allowing for a comprehensive analysis of the relationship between IoT implementation and SCRM. It provides a structured approach to examining the various components of IoT systems, such as the sensing layer, service and interface layer, and data processing layer, and their implications for SCRM processes.

DISCUSSION

To comprehensively address the research topic and investigate key relevant research disciplines, several areas can be explored in relation to the implications of IoT on supply chain risk management (SCRM). Here are some important disciplines that can be considered:

Development of “supply chain risk management” through the application of the “Internet of Things”

The integration of IoT in SCRM enables real-time data collection and processing, which facilitates the identification of potential risks. This aligns with the findings in the literature and presents a novel research topic within the framework of IPT. By leveraging self-acting algorithms and real-time data, IoT enhances risk management capabilities by providing timely information on both operational and strategic risks. In the context of SCRM, the use of standardized process structures supported the successful identification of micro risks through the comparison of real-time data with predefined criteria. However, to uncover a broader range of risks and improve decision-making, it is important to incorporate additional data sources such as newspaper articles, weather data, or market prices. By incorporating these diverse data sources, SCRM practitioners can enhance their ability to prioritize risks effectively. The combination of real-time data, self-acting algorithms, and supplementary information sources empowers organizations to make more informed decisions regarding risk mitigation and allocation of resources. Overall, the utilization of IoT in SCRM opens up new possibilities for risk management by leveraging advanced data analytics and information exchange capabilities. This research direction holds significant potential for further exploration and contributes to the ongoing understanding of how IoT can transform SCRM practices.

Effects on the internal and external pathway

The successful implementation and utilization of information processing systems in SCRM involve various factors, including technical considerations as well as cultural, psychological, and strategic aspects. It is crucial to evaluate both internal and external factors that contribute to success before implementing such systems and to initiate organizational changes accordingly. One internal factor that can impact the adoption of new technology is employee resistance, which may stem from fear of change, concerns about job security, or unfamiliarity with new work practices. However, our findings suggest that these concerns may be unfounded, as the introduction of IoT in SCRM can actually support

employees and alleviate tedious tasks, leading to increased job satisfaction. Cultural factors, such as a learning orientation, have been identified as significant drivers for internal system implementation. A culture characterized by a commitment to learning, a shared vision, and an open-minded attitude fosters a conducive environment for the successful adoption and integration of information processing systems. The propagation of SCRM culture, team support, and alignment with SCRM strategy have also been found to be important factors in implementing SCRM information systems. It is worth noting that the specific patterns of behavior related to cultural factors may vary across organizations, including factors such as the organization's size, SCRM structure, and product specificities. However, the overall organizational culture and individual employees should be taken into account when implementing information processing systems in SCRM. Front-line employees, in particular, can play a critical role as they are often the first to identify suspicious situations and potential threats. To ensure successful implementation and adoption of information processing systems in SCRM, organizations should address cultural factors, provide support to employees, and consider the specific dynamics of their own organizational context. By fostering a supportive culture and engaging employees in the implementation process, organizations can enhance the effectiveness and acceptance of information processing systems in SCRM.

Effects on the supply chain risk management outcomes and barriers to overcome

The literature supports the idea that technological and creative capabilities can enhance SCRM results and organizational performance. Our case study findings align with this notion, as the implementation of IoT in SCRM can improve information availability and process management, leading to a better alignment between increasing information capabilities and processing capacity. This, in turn, can contribute to improved SCRM outcomes and overall organizational performance. However, our study also revealed certain challenges that need to be addressed for successful IoT system deployment. Technical and financial aspects, such as the availability of complete infrastructure and high error rates in automatically generated risk alerts, were mentioned as important considerations by the respondents. These concerns highlight the need to carefully evaluate the devices used for creating algorithms and the IoT devices themselves, as well as the infrastructure supporting their operation. Despite the ongoing advancements in technology and the decreasing costs associated with IoT implementation, these aspects remain crucial considerations for practitioners. The literature findings, as well as our case study, emphasize the importance of addressing these technical and financial challenges to ensure the successful deployment and utilization of IoT systems in SCRM. By recognizing and addressing these concerns, organizations can better leverage the potential benefits of IoT in SCRM, mitigate risks associated with incomplete infrastructure or high error rates, and maximize the positive impact of technological and creative capabilities on SCRM outcomes and organizational performance.

CONCLUSION

The complex nature of business environments, characterized by pressure, rapid product cycles, and volatility, highlights the importance of SCRM supported by technological innovations such as IoT. Our study fills a research gap by conducting multiple case studies to gain real-world insights, guided by a theoretically based research approach, to assess the influence of IoT on SCRM. Through our case study observations, we provide practical insights into the structure of IoT and derive propositions regarding its impact on data availability, process management, specific process stages, internal and external routes, and SCRM outcomes. As a result, our research contributes to the existing body of knowledge while offering fresh insights for practitioners, highlighting the transformative potential of IoT in supply chain risk management. IoT enables rapid access to real-time information from a wide range of sources, enhancing risk transparency. Additionally, the ability to integrate systems allows for increased automation, accelerating processes and facilitating the evaluation and analysis of large volumes of data. Beyond process optimization, IoT significantly influences risk management, job roles, and corporate culture. It enhances sourcing processes and supplier selection, which are critical sources of risk in the supply chain. The use of IoT enables quick, reliable, and cost-effective assessment of suppliers and related processes, facilitating on going audits and reducing ambiguity. However, challenges such as complex data management, assessing profitability, and resistance from individuals need to be effectively addressed. These challenges open up numerous avenues for further research and present an excellent opportunity to make significant contributions to the field. Despite the valuable contribution of our research, it is important to acknowledge the limitations of our empirical research approach.

The case study technique, while suitable for exploratory research, has limitations in terms of generalizability due to its reliance on the observed sample and the novelty of the research subject. Therefore, it is recommended to investigate

additional industries and conduct more interviews to validate claims within organizations. Exploring specific relationships between suppliers and customers within one component of the supply chain can provide a deeper understanding of IoT's impact on the industry. Furthermore, conducting large-scale empirical studies using cross-sectional data across multiple sectors would help validate the research findings. Considering organizations engaged in SCRM interactions would also yield additional insights. Overall, by addressing these limitations and exploring further research avenues, we can continue to advance our understanding of the impacts of IoT on SCRM, benefiting both practitioners and academics in the field.

REFERENCES

Al-Ayed, S. I. and Al-Tit, A. A. (2023) 'The effect of supply chain risk management on supply chain resilience: The intervening part of Internet-of-Things', Uncertain Supply Chain Management, 11(1), pp. 179–186. doi: 10.5267/j.uscm.2022.10.009.

Aven, T. (2016) 'Risk assessment and risk management: Review of recent advances on their foundation', European Journal of Operational Research, 253(1), pp. 1–13. doi: 10.1016/j.ejor.2015.12.023.

Aven, T. et al. (2020) 'Risk assessment and risk management: Review of recent advances on their foundation', Industrial Management and Data Systems, 118(3), pp. 1–13. doi: 10.5267/j.uscm.2022.10.009.

Bedard, J. C. et al. (2008) 'Risk monitoring and control in audit firms: A research synthesis', Auditing, 27(1), pp. 187–218. doi: 10.2308/aud.2008.27.1.187.

Birkel, H. S. and Hartmann, E. (2020) 'Internet of Things – the future of managing supply chain risks', Supply Chain Management, 25(5), pp. 535–548. doi: 10.1108/SCM-09-2019-0356.

Eisenhardt, K. M. et al. (2020) 'Risk assessment and risk management: Review of recent advances on their foundation', Industrial Management and Data Systems, 8(3), pp. 1–13. doi: 10.5267/j.uscm.2022.10.009.

Fan, H. et al. (2017) 'An information processing perspective on supply chain risk management: Antecedents, mechanism, and consequences', International Journal of Production Economics, 185, pp. 63–75. doi: 10.1016/j.ijpe.2016.11.015.

Gold, S. and Schleper, M. C. (2017) 'A pathway towards true sustainability: A recognition foundation of sustainable supply chain management', European Management Journal, 35(4), pp. 425–429. doi: 10.1016/j.emj.2017.06.008.

Harsasi, M. and Minrohayati (2017) 'The impact of supply chain management practices on competitive advantage', International Journal of Economic Policy in Emerging Economies, 10(3), pp. 240–247. doi: 10.1504/IJEPEE.2017.086623.

Hiromoto, R. E., Haney, M. and Vakanski, A. (2017) 'A secure architecture for IoT with supply chain risk management', Proceedings of the 2017 IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2017, 1(January 2020), pp. 431–435. doi: 10.1109/IDAACS.2017.8095118.

Kayis, E., Erhun, F. and Plambeck, E. L. (2013) 'Delegation vs. control of component procurement under asymmetric cost information and simple contracts', Manufacturing and Service Operations Management, 15(1), pp. 45–56. doi: 10.1287/msom.1120.0395.

Kieras, T., Farooq, J. and Zhu, Q. (2021) 'I-SCRAM: A Framework for IoT Supply Chain Risk Analysis and Mitigation Decisions', IEEE Access, 9, pp. 29827–29840. doi: 10.1109/ACCESS.2021.3058338.

Kothari, S. S., Jain, S. V and Venkteshwar, P. A. (2018) 'The Impact of IOT in Supply Chain Management', International Research Journal of Engineering and Technology (IRJET), pp. 257–259.

Kotzab, H. et al. (2015) 'Supply chain management resources, capabilities and execution', Production Planning and Control, 26(7), pp. 525–542. doi: 10.1080/09537287.2014.927932.

Manuj, I. and Mentzer, J. T. (2008) 'Global supply chain risk management strategies', International Journal of Physical Distribution and Logistics Management, 38(3), pp. 192–223. doi: 10.1108/09600030810866986.

Noor, M. A., Khalfan, M. M. A. and Maqsood, T. (2013) 'The role of procurement practices in effective implementation of infrastructure projects in Pakistan', International Journal of Managing Projects in Business, 6(4), pp. 802–826. doi: 10.1108/IJMPB-03-2012-0005.

Purdy, G. (2010) 'ISO 31000:2009 - Setting a new standard for risk management: Perspective', Risk Analysis, 30(6), pp.

881–886. doi: 10.1111/j.1539-6924.2010.01442.x.

Tchankova, L. (2002) 'Risk identification – basic stage in risk management', Environmental Management and Health, 13(3), pp. 290–297. doi: 10.1108/09566160210431088.

Tsang, Y. P. et al. (2018) 'An Internet of Things (IoT)-based risk monitoring system for managing cold supply chain risks', Industrial Management and Data Systems, 118(7), pp. 1432–1462. doi: 10.1108/IMDS-09-2017-0384.