Knowledge Risks in Digital Supply Chains: A Literature Review

Johannes Paul Zeiringer[1] and Stefan Thalmann[1]

[1] University of Graz, Business Analytics and Data Science-Center, Graz, Austria
johannes.zeiringer@uni-graz.at, stefan.thalmann@uni-graz.at

Abstract. The digital transformation changes the way how organizations exchange data in supply chains. Data traditionally shared, is enriched by detailed data sets captured by sensors in the production itself. In addition to the promised benefits, also new risks arise. Advanced data analytic approaches make it possible to extract knowledge from such data sets and thus increase the risk that competitive knowledge unintentionally spills over. From a knowledge management perspective, little attention is paid to such knowledge risks arising from data-centric collaborations. Hence, this paper has the goal to investigate knowledge risks in data-centric collaborations by conducting a structured literature review. Thereby, we focus on digital supply chains, as data-centric collaborations play a central role within them. Based on our review, we identify four characteristics of digital supply chains relevant for managing knowledge risks. Based on these characteristics, we present causes, risks and countermeasures from an organizational, technical and legal perspective.

Keywords: Knowledge Protection, Digital Supply Chain, Knowledge Risks, Data-centric Collaboration

1 Introduction

The digital transformation changes the way how data and knowledge is shared in inter-organizational supply chains (SC). From a knowledge management (KM) perspective, inter-organizational knowledge sharing has a strategic dimension and requires a careful balancing of knowledge sharing and protection [1]. Regarding the knowledge sharing, corporations increasingly rely on the know-how and expertise of external organizations for SC innovation and SC improvements [2]. This increasing exchange of comprehensive data sets, however, poses new knowledge risks [3].

So far, KM research focuses mainly on knowledge sharing and protection between persons (representing organizations) in the form of implicit and explicit knowledge exchange. Little is known about knowledge risks arising from knowledge discovery of huge and comprehensive data sets shared in the course of their digital SC [3], [4]. Data exchange in SC is not new, but due to the digitalization the scope and the nature changed. Traditionally, data for order management and logistics management are exchanged in clearly specified ways. Advanced concepts of digitalization such as Industry 4.0 or smart manufacturing, however, require a more comprehensive

15th International Conference on Wirtschaftsinformatik,
March 08-11, 2020, Potsdam, Germany

https://doi.org/10.30844/wi_2020_d1-zeiringer

exchange of production data [5], [6]. These data sets are collected by new sensors combined with Internet of Things (IoT) technology to increase SC efficiency [7]. Current research shows that data-centric collaborations pose new knowledge risks and that existing KM literature has no suitable answers yet [8], [2]. However, risk management (RM) in general is a central part of supply chain management (SCM) and a promising starting point for investigating knowledge risks in data-centric collaborations. Based on this observation the authors want to answer the following research question (RQ):

Which kind of knowledge risks arise from data-centric collaborations and what are suitable countermeasures?

To answer the RQ, a structured literature review according to [9] will be performed. The review focuses on SCM, as digitalized SC are the most prominent example for data-centric collaborations and SCM has a long tradition of applying RM.

2 Background

2.1 Digitalization

Digitization in industry started in the 1980s with focus on logistic and order management. Information systems (IS) improved during the 1990s and demand information have already been shared along the SC at this time, in a controllable and manageable manner [10]. As it can be seen, data has been exchanged for decades, but data as a primary reason of interest within the SC is relatively new [11].

The digital transformation is seen as a process that induces digital technologies which, in further consequence, lead to disruptions [7]. This has led to many innovations and changes in different industry sectors and affects SCM. Efficiency is one of the core aspects in SCM, which can be further pushed in a digitized industry [5]. Such improvement attempts are known as concepts like Industry 4.0, smart factories or smart manufacturing and influence SC processes nowadays [12]. Digitalization is not only penetrating SC increasingly but also, more and more firms are inter-organizational connected and share data about more and more topics along the SC [13], [4].

Digitalization bases on a manufacturing model in which machinery and products automatically exchange comprehensive data sets without human command. High degrees of customization and flexible processes on the SC level are key advantages[12], [14]. Enhanced data collection, transfer and analytics capabilities are the backbone of digitalization and essential to realize the level of flexibility without significant drawbacks on quality or costs. As a result, industry is therefore transforming into an automated high-tech environment with excessive data sharing and SC are digitalized [5].

https://doi.org/10.30844/wi_2020_d1-zeiringer

2.2 Digital Supply Chain

Digitalization enhances the number of connected devices intensely. Implementation of advanced digital technologies (e.g. IoT or Artificial Intelligence (AI)) determine the digital SC. Sensors in industrial ecosystems control and monitor processes of industrial production and, as part of it, generate and share data continuously [15]. The digital SC includes systems that facilitate the interaction between organizations and orchestrate SC partners [16]. Organizations are becoming more and more integrated in digital SC leading to better performance and competitiveness of the SC and organization [17]. Data is a key asset in SC and a source to support SC activities. The goal of data-centric collaborations is to minimize the manual intervention in SC processes to improve safety, efficiency and sustainability through automation. With modern data science approaches, comprehensive data sets, collected from industrial ecosystems, can be continuously analysed to gain useful knowledge for industrial automation [15], [18].

Conclusively, we define the digital SC as a highly integrated and multilayered production network which can be optimized and (re)composed flexibly and quickly.

2.3 Supply Chain Risk Management (SCRM)

One of the major challenges for management is to predict, raise consciousness, analyze, monitor and handle risks. As SC are highly sensitive networks involving many actors and having an interwoven nature, RM has always a high priority, e.g. [19], [20]. SCRM is defined as an inter-organizational collaborative effort using quantitative and qualitative RM methodologies to identify, evaluate, mitigate and monitor if unexpected events or conditions could adversely affect any part of the SC [20], [21].

SC risk defines challenges linked to potential disturbances influencing SC partners that may directly influence the capacity of a company to operate, sell products, or offer customer services [22]. Effective SCRM relies on collaboration, and is the key to the general success of the SC [23]. As mentioned in 2.1, digitalization changes SC, generates new chances but also new risks in cyber-space, and leads to cyber SCRM. Organizations need support in understanding and improving RM and cyber resilience in their digital SC. In the management of cyber and information risk, there is merely SC view in current scientific contributions, but no knowledge protection view [24].

2.4 Knowledge Management in Data-centric Collaborations

KM in SC primarily focuses on inter-organizational knowledge sharing. From this perspective, the balancing of measures fostering knowledge sharing between SC partners and measures protecting knowledge is a central task [1], [25], [26]. Despite knowledge protection being a core strategy of KM [27], it is mainly investigated on a conceptual level for explicit knowledge in formal settings [28]. In this regard, legal (contractual) as well as technical (access control) measures are discussed [29].

https://doi.org/10.30844/wi_2020_d1-zeiringer

As digital transformation blurs the line between different manifestations of knowledge, data-centric collaborations become relevant from a knowledge protection point of view as well [3]. However, from an KM perspective this topic received little attention so far.

Collaboration involves the exchange of data, and therefore knowledge risks emerge, especially in data-centric collaborations. Unless these risks are eliminated or managed, they leave a company fragile. Furthermore, scholars show that competitive pressures, cost shifting, information asymmetry and privacy, and path dependencies stop data-centric collaborations from being taken up [17], [13].

3 Procedure

To answer the RQ, a structured literature review was conducted. The authors followed the approach proposed by Webster and Watson [9]. This work consists of a structured review of 40 scientific papers. The papers were gathered by determining three key parameters at first: keywords, relevant journals and conference proceedings, and the time of publishing. Regarding the keywords, the authors defined keywords representing each of the most important domains (i.e. SCM, KM, IS and Strategic Management). The respective keywords were concatenated into scope of the search in towards the goal of the literature review (see Appendix 1).

The authors focused on key journals of every of the relevant four domains to investigate the best publications in a rigorous way [9]. For an overview of the considered journals, a matrix (see Appendix 1) was categorized in domains based on the VHB[1] categories. The timespan for sources was set from 2010-2019. Since data-centered collaborations and digital SC are concepts of this decade, the time span has been adapted as such [5].

The search was performed in “google scholar” and “Web of Science”. Papers were selected according to the following conditions: “if paper has two primary keys or at least one primary and at least one secondary key”. This was applied to title and keywords. An example for combined keywords reads as follows: "data exchange" AND "supply chain" AND "digitalization" AND “security”. In the given example “data exchange” and “supply chain” are primary keywords and “digitalization” and “security” are secondary ones (see Appendix 1). The search led to 116 papers in total.

If this restriction was met, the abstract was first scanned and checked for relevance before the paper was transferred to the matrix created. The abstract proved to be relevant, if the topics of SCM in combination with KM or RM or digitalization were addressed. Further, a paper proved to be relevant if, e.g., it dealt with knowledge protection in the digital area, such as cyber security, and not with knowledge protection in the event of employee turnover within the SC. After the abstract scan 47 papers remained. Those were analyzed with the qualitative content analysis [30]. In this examination, it appeared that there are still papers not helping to answer the RQ and were therefore excluded. Overall 17 papers were excluded, and the number of

[1] Verband der Hochschullehrer für Betriebswirtschaft (2019), https://vhbonline.org/startseite/

https://doi.org/10.30844/wi_2020_d1-zeiringer

useful papers was reduced to 30. The authors paid close attention to whether the risks are mere traditional SCM risks in collaborations or can also be considered as knowledge risks in data-centric collaborations. As an example of a non-knowledge risk, the authors note natural accidents, like fire or earthquakes [31]. Finally, the 30 papers were used for a forward-/backward-scan with "Scopus" to find another 10 papers. In total, 40 papers were left for reviewing.

We analyzed the 40 papers by applying the structured content analysis according to Mayring [30]. The first step was to summarize the papers and then to structure them according the dimensions organizational, technical and legal. Furthermore, the focus was on causes for risks, identifying risks and possible countermeasures and characteristics of digital SC. Afterwards, the results were interpreted and synthesized in a concept-centric way, as proposed by Webster & Watson [9].

4 Discussion of Results

4.1 Characteristics of the Digital Supply Chain.

Within the literature review, four key characteristics of digital SC were identified which are relevant from a knowledge risk perspective: (1) more and more comprehensive data sets are exchanged, (2) the IT penetration and the dependency on IT systems increased, (3) the SC are more frequently changed and composed differently and (4) there is only a limited transparency and relational capital between SC partners. In the following these characteristics will be discussed.

(1) Disruptive technologies, such as IoT or AI have an impact on reorganizing SC. With the use of cyber-physical system concepts, new production approaches are possible, focusing on highly customized assembly technologies with flexible process design. Cyber physical systems, smart, in real time connected products and advanced data storage and processing capabilities encourage digital SC and the introduction of smart processes, e.g. [5], [12]. As a result, more and more data is generated, which is also exchanged between the partners. Furthermore, data sets become more comprehensive as IoT and cheaper sensors boost the data capturing within the manufacturing process [14], [6]. Data analysis is a key aspect in digital SC, in order to enhance efficiency [32].

(2) The above described datafication and the digitalization in general demand new IT-approaches for highly integrated networks, e.g. [12], [33]. Such highly integrated networks together with cyber physical system and smart, in real time connected products, increase the IT penetration in SC. This increased IT penetration also leads to a higher dependency and increases the risk of cyber vulnerabilities, e.g. [24], [34]. Both demands for advanced IT risk management and an increased need for IT-knowledge.

(3) Trends like mass customization, lot size 1 approaches and shorter product life cycles, lead to an expanding complexity within digital SC, which are multi-layer, multi-supplier, multi-commodity and multi-channel, e.g. [13], [34]. Consequently, SC are more frequently changed and composed differently. Also, controlling data in a

https://doi.org/10.30844/wi_2020_d1-zeiringer

digital SC cannot be restricted to a single area that is governed by a single organization, as it does not lie within the borders of a single organization [16], [35]. Hence, this increased dynamic challenges traditional approaches of SCRM.

(4) Another consequence of more flexible compositions of SC networks is that SC partners are increasingly involved, without knowing each other, leading to lower relational capital and lower levels of trust between SC partners. This is especially true for indirect ties in multilayered SC networks leading to a lack of transparency and the question who shares what kind of data with whom, e.g. [34], [24], [36].

4.2 Organizational View

Causes for Risks. From an organizational perspective, scholars report about the lack of communication or information asymmetry, e.g. [37], [13], [38], [39]. Information asymmetry because of limited information in single firms leads to barriers of sharing and resistance. First, this resistance can lead to non-adoption of digital SC and second, more barriers for communication among SC actors to less transparency. The first, because it is difficult to keep track of the amount of the exchanged data, and cyber-attacks and other security risks are threatening the organization. IT penetration and the dependency on IT systems require more IT-knowledge within the company. A non-compliance of these requirements leads to risks, e.g. [13], [37].

Regarding the second, if there is no social relationship between partners, a general lack of communication appears. This causes a lack of trust between partners, decreasing the commitment to share sensitive information and increasing the need for complex contracts to protect interests, e.g. [37], [40]. Together with the high fluctuation between partners, the transparency, needed for a solid risk assessment, is limited. This even leads to an intensification of the lack of trust.

Identified Risks. Extensive sharing of data can result in the loss or theft of intellectual property (IP), e.g. [41], [37]. In this regard, a substantial risk is the intentional or non-intentional leakage of knowledge as well as potential ill-will by insiders and outsiders, e.g. [42], [36], [31]. These challenges go hand in hand with a lack of trust and lack of communication, and become even more challenging with more frequently changed partners and less relational capital within the digital SC. Therefore, it is important for firms to be aware of potential consequences and what data is shared through the entire SC, e.g. [34], [16].

Furthermore, it might be said that employees potentially do not have the IT-competences to monitor which knowledge can be extracted from the data leaving the company and are averse to engage in collaborations. This is especially relevant for digital SC. As there is always a need for sharing and for protection of knowledge, the right balance needs to be found.

Countermeasures. Management strategies are needed to face the risks of increased data exchange in digital SC. Proactive management strategy aims to detect risky incidents and deter loss by analyzing critical situations. This should reduce the probability of undesirable risk by implementing preventive measures. It is shown that proactive risk assessment makes SCRM more robust. Reactive management consists

https://doi.org/10.30844/wi_2020_d1-zeiringer

of corrective measures to reduce the effects of undesired risk incidents. This needs responsiveness and good knowledge of all available options and their impact on the efficiency of the SC, e.g. [43], [24], [12].

Due to the flexibility of digital SC and the reduced relational capital between SC partners, it is also necessary to define and apply explicit and common collaboration rules. Additionally, a collaborative business culture needs to be established in broader SC network to ensure a good collaboration. Partner selection is crucial in SCM, and becomes more difficult in digital SC. Furthermore, organizational and personal learning, including knowledge transfer, and internal and external awareness training are meaningful countermeasures for knowledge risks, especially with regards to the increased penetration of IT systems and dependency in digital SC, e.g. [13], [23], [44], [36], [45], [46], [16]. Also, decision support systems can be useful tools to support KM and facilitate collaborative learning within the digital SC [47].

The results show that in case of a lack of communication or trust, stakeholders might be reluctant to collaborate in a digital SC. Reasons for this are more frequently changed compositions of SC partners and the limited relational capital among them. Furthermore, if network partners do not know, what kind of data is leaving the company the intentional or non-intentional knowledge leakage is urgent. It is crucial to be aware what data is exchanged, otherwise the attitude towards data-centric collaborations is shrinking within the organization. Hence, it can be assumed that both proactive and reactive management strategies, as well as common collaborations rules are essential.

4.3 Technical View

Causes for Risks. As the IT dependency increases (see 2.1), a company must be technically up to date and be able to adapt to technological changes. If there is an inadequate business process reengineering, a lack of concurrent design, an inadequate IT-system, or lax IT security, there is always a higher possibility for a risk, like a cyber-attack or data theft, e.g. [38], [36].

Further causes for risks are the absence of a performance measuring system, absence of a conflict resolution procedure, a missing contingency plan, or a lack of access restriction, e.g. [12], [48]. These considerations apply in particular to data-centric companies that rely on high-tech infrastructure and exchange vast amounts of data sets in an automated way. Along with the increased penetration of IT systems and smart objects, cyber-attacks become more likely [13], [24].

As mentioned above, an adequate IT system is crucial. Low level safety technologies lead to the possible emergence of a risk, e.g. [34], [41], [40]. This cause even increases with frequently changing SC partners and limited transparency.

Identified Risks. More and more comprehensive data sets are shared in digital SC and it is difficult for companies to be aware of which knowledge can be extracted out of such data sets. It is shown that reverse engineering can be a possible threat to firms' intellectual property, e.g. [41], [49]. With modern data analytics approaches, it is possible to extract knowledge by analyzing exchanged data within the SC. Sensor

https://doi.org/10.30844/wi_2020_d1-zeiringer

data is generated constantly in IoT networks, making data sets much more comprehensive [50]. Hence, deciders should be able to assess the risks related to specific data items while balancing between benefits of sharing and the risks associated with the data. Further, it should be mentioned that it is not always clear for which purposes shared data sets and items are used by SC partners. Additionally, there is a security and privacy risk, which increases with the dependency on IT, e.g. [36], [24], [51], [11].

Information security is one of the most important aspects within a SC. If a company loses private information related to its SC, it may adversely affect future contractual decisions with its partners. It also seriously threatens to lose business and future alliances with potential customers or suppliers. Many companies have attempted to reduce their providers and establish better relationships with main partners, in the aim of establishing a secure infrastructure and of preventing unauthorized persons from disclosure, e.g. [35], [34], [13]. Another way is to implement auditing procedures [52].

Countermeasures. Technical countermeasures focus on security architectures, securing the transmission of information, on cryptography and on monitoring data streams. Data management and IT security tools support the management, pattern and anomaly detection based on real-time data from sensors, or data flows can be used as countermeasures, e.g. [16], [44], [24], [39], [53], [34], [42], [54], [55].

Another approach is the association rule hiding, which aims at avoiding risks that are caused by knowledge leakage by removing sensitive association rules from the database before they are shared [42]. Using predictive analytics for predictive maintenance and forecasting helps SC to become more robust to disruptions, e.g. [13], [54], [19]. Also, businesses should take benefit of advanced IT systems, using the vast quantity of information that is accessible within the SC, in order to make automated decisions, e.g. [53], [47], [37].

From a technical point of view, knowledge risks in data-centric collaborations are based on similar risks as in the traditional SC collaboration. An inadequate IT-system, lax IT security or low-level safety technologies contribute to emerging risks. However, the knowledge extraction out of larger and more comprehensive data sets is an upcoming challenge. In a frequently changing SC with only a limited transparency between partners, effective IT measures are needed as to protect knowledge.

4.4 Legal View

Causes for Risks. Breaches of data security and privacy agreements by SC partners or employees lead to risks. Hence, it is crucial to be aware of who is legally allowed to access machine generated data. As data is not scarce, it can be copied and multiplied without restricting others. This leads to the challenge that it is difficult to assign ownerships of the data and that classical IP law cannot be applied, e.g. [33], [56].

The unclear ownership of rights to aggregated know-how, and technical data, due to employee turnover, can lead to risks as well [33]. This could not only affect

https://doi.org/10.30844/wi_2020_d1-zeiringer

employee turnover but also changing partners and limited transparency within the digital SC.

SC partners can extract competitive knowledge out of the shared data sets. As data is shared for the purposes of operating and optimizing the SC, e.g. quality management, it is not clear how to deal with such unintended use from a legal perspective. This is particularly the case, as it is difficult to trace who is making use of shared data in which way and is tied to the limited transparency between SC partners. One resulting question is, if manufacturers of smart objects do have access to the generated data and how contracts are adapted to modern requirements [33].

If there is too much confidentiality, the knowledge exchange suffers, and partners are put at a competitive disadvantage. Also, there is a need for anti-trust regulations by the state to ensure fair competition and prevent emerging risks, e.g. [40], [36].

Identified Risks. These causes for risks mentioned above can lead to the unintended leakage of competitive knowledge, which represents a legal challenge, e.g., [41], [36], [40]. Since there is no clear data ownership protection in the EU, the question of who the legal owner of data is, is not clearly answered in the legal framework of the EU. As already mentioned, formal legal protection measures for process knowledge are limited and machine-generated data therefore presents a risk. How legal measures can be enforced towards this challenge remains to be clarified [33].

Patents are usually not a suitable measure. First, they are less suitable for process knowledge, second, if sensible knowledge is patented, it needs to be disclosed and third, patents and especially enforcement of patents is challenging for SMEs [52].

Countermeasures. From a legal point of view, formal contracts are meaningful countermeasures. To avoid emerging risks, a contract management embedded in the SC network is essential, especially in frequently changing SC networks with only a limited transparency and relational capital, e.g. [16], [21]. As already mentioned, patents can be a countermeasure, but they are not always adequate and firms often use secrecy or lead time advantage to protect their process knowledge, e.g. [57], [38], [52].

IP can be protected by formal and informal measures, like trade secrets, copyright protection or patent protection. Regarding industry 4.0 new approaches are needed to protect process knowledge. In data-centric collaborations, it is important that contractual agreements consider the data exchange and non-disclosure agreements are used. Within these contracts, details about gathering and using of data are essential [33].

Due to the restrictive nature of the search, only a few legal points could be identified. In this context, a focus must be placed on further research. Legal risks, regarding knowledge protection in data-centric collaborations are similar to those in traditional collaborations. There is also a need for formal and legal contracts and a strict contract management, especially regarding the characteristics of digital SC.

Table 1 synthesizes existing challenges and countermeasures with suitable approaches for the digital SC.

Table 1: Challenges and possible countermeasures for characteristics in digital SC

https://doi.org/10.30844/wi_2020_d1-zeiringer

Characteristics (see 2.1)	Challenges for Digital SC	Countermeasures for Digital SC
(1)	• intentional or non-intentional leakage of data • no transparency about knowledge in shared data sets • difficult to assign ownerships of the data • theft of data or intellectual property	• decision support tools for shared data sets • securing the transmission of information, cryptography • explicit collaboration rules and procurement conditions • organizational and personal learning and training
(2)	• no proper IT-training & instruction • no proper IT-systems, low-level safety technologies • security and privacy issues, cyber-attacks, theft of IP • dealing with sensor data	• modern IT systems • securing the transmission of data, cryptography • organizational and personal learning and training • knowledge based access control for data sets
(3)	• no social relationships, lack of trust • increasing complexity of modern SC • breaches of data security and privacy by SC partners	• controlled information sharing in trusted domains • standardization of procedures, joint decision-making • develop collaborative business culture in firms • legal contracts, KM
(4)	• lack of communication, trust & partner commitment • breaches of data security and privacy by SC partners • difficult to assign ownerships of the data • increasing complexity of modern SC	• controlled information sharing in trusted domains • standardization of procedures, joint decision-making • develop collaborative business culture in firms • legal contracts, KM

4.5 Avenues for future research.

Challenges regarding knowledge protection within a SC are nothing new, but due to digitalization new challenges arise. Based on our structured literature review we discuss promising avenues for future research.

Organizational view. First of all, it is important to state, that measures for raising awareness on new emerging knowledge risks are needed. Building trusted relationships is important in digital SC as well. However, new forms of trust building are needed, as the exchange of knowledge happens without human interaction and it is difficult to keep track of the exchanged data sets. Therefore, it is important to define clear instructions on sharing which data with whom to reduce insecurities within the organization and to define clear collaboration rules. Also, research on strategies how to balance sharing and protection is needed and finally similarly to security action plans for what to do after an incident need to be defined [58].

Technical view. The review showed that technical measures primary focus on IT security. However, securing the data transfer itself is not the major issue, rather than deciding on which data, including which knowledge, should be shared. Hence, research is needed on how to provide decision makers a suitable decision basis (as they currently cannot answer the question properly which knowledge can be discovered out of a data set) and therefore allow an effective enforcement of knowledge protection. In this regard, decision support tools identifying potential knowledge risks or technical measures such as synthetic data sets to anonymize the exchanged data and retain confidentiality seem promising.

Legal view. The ownership, and therefore possible utilization of data is one of the most urgent challenges within the digital SC. As well as the depth of the digital SC as

https://doi.org/10.30844/wi_2020_d1-zeiringer

cross-border relations intensify this problem even more. It is difficult to enforce legal measures cross-border, even throughout the EU and especially globally. Furthermore, it is to be assumed that assignment obligations alone are not sufficient. The need for new collaboration contracts is given.

5 Conclusion

Due to IT, information and services in network infrastructures, production technologies and SC are becoming more connected, faster and more efficient. All this involves a growing need to share larger and more comprehensive data sets from which competitive knowledge could be discovered. As a result, a new category of knowledge risks is emerging. This in return demands an appropriate strategy to knowledge protection taking data-centric collaborations into account. Although it is commonly recognized that sharing data can make SC operations more efficient, it is less known that sharing data can also promote RM and mitigation of disruptions for the creation of stable and resilient SC if used correctly, e.g. [34], [59].

In digital SC, four characteristics were stated: (1) more and more comprehensive data sets are exchanged, (2) the IT penetration and the dependency on IT systems increased, (3) the SC are more frequently changed and composed differently and (4) there is only a limited transparency and relational capital between SC partners. Due to these characteristics, a loss of control is possible and malicious assaults like hacker activities are more likely to occur. Overall, the literature review shows that it is difficult to isolate risks making their management challenging. Therefore, securing data is crucial, as well as proper RM, e.g. [34], [39], [42].

Based on this, the authors can conclude that transparency on the risks is desired from the organizational perspective. Only if employees know what others can discover from data sets, they can decide best and balance benefits and risks in a sharing decision. From a technical perspective, new approaches are needed to not only control the data flow itself, but also to control which knowledge is included in the data. From a legal perspective, new approaches are needed to deal with the unintended analysis of data by other SC partners.

One of the main insights of this review is that there is little research regarding the field of knowledge risks in data-centric collaborations, which indicates that there is a demand for further research on this drawback of digitalization. Furthermore, data-centric collaboration itself is not adequately dealt with so far, as there is still a focus on traditional risks and hardly on intangible risks. There is need for a knowledge protection framework and in future research the authors intend to investigate which kind of measures are meaningful to balance knowledge sharing and protection.

References

1. Loebbecke, C., van Fenema, P.C., Powell, P.: Managing inter-organizational knowledge sharing. The Journal of Strategic Information Systems 25, 4–14 (2016)

https://doi.org/10.30844/wi_2020_d1-zeiringer

2. Zacharia, Z., Plasch, M., Mohan, U., Gerschberger, M.: The emerging role of coopetition within inter-firm relationships. Int Jrnl Logistics Management 30, 414–437 (2019)
3. Ilvonen, I., Thalmann, S., Manhart, M., Sillaber, C.: Reconciling digital transformation and knowledge protection: a research agenda. Knowledge Management Research & Practice 16, 235–244 (2018)
4. North, K., Carvalho, A. de, Braccini, A., Durst, S., Carvalho, J., Gräslund, K., Thalmann, S.: Information and knowledge risks in supply chain interactions of SMEs. Proceedings of the 10th International Conference on Practical Knowledge Management, Potsdam, Germany. Lecture notes on Informatics. (2019)
5. Kagermann, H.: Change Through Digitization—Value Creation in the Age of Industry 4.0. In: Albach, H., Meffert, H., Pinkwart, A., Reichwald, R. (eds.) Management of Permanent Change, pp. 23–45. Springer Fachmedien Wiesbaden, Wiesbaden (2015)
6. Schniederjans, D.G., Curado, C., Khalajhedayati, M.: Supply chain digitisation trends: An integration of knowledge management. International Journal of Production Economics, 107439 (2019)
7. Vial, G.: Understanding digital transformation: A review and a research agenda. The Journal of Strategic Information Systems 28, 118–144 (2019)
8. Rene Kaiser, Stefan Thalmann, Viktoria Pammer-Schindler and Angela Fessl: Collaborating in a Research and Development Project: Knowledge Protection Practices applied in a Co-opetitive Setting. ", Proceedings of the 10th International Conference on Practical Knowledge Management, Potsdam, Germany. Lecture notes on Informatics. (2019)
9. Webster, J., Watson, R.: Analyzing the Past to Prepare for the Future: Writing a Literature Review. MIS Quarterly 26 (2002)
10. Min, S., Zacharia, Z.G., Smith, C.D.: Defining Supply Chain Management: In the Past, Present, and Future. J Bus Logist 40, 44–55 (2019)
11. Spanaki, K., Gürgüç, Z., Adams, R., Mulligan, C.: Data supply chain (DSC): research synthesis and future directions. International Journal of Production Research 56, 4447–4466 (2018)
12. Ivanov, D., Dolgui, A., Sokolov, B.: The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. International Journal of Production Research 57, 829–846 (2019)
13. Kazantsev, N., Pishchulov, G., Mehandjiev, N., Sampaio, P., Zolkiewski, J.: Formation of Demand-Driven Collaborations between Suppliers in Industry 4.0 Production Networks. 20th International Working Seminar on Production Economics (2018)
14. Malte Brettel, Niklas Friederichsen, Michael Keller, Marius Rosenberg: How Virtualization, Decentralization and Network Building Change the Manufacturing Landscape: An Industry 4.0 Perspective
15. Chen, Y., Lee, G.M., Shu, L., Crespi, N.: Industrial Internet of Things-Based Collaborative Sensing Intelligence: Framework and Research Challenges. Sensors (Basel, Switzerland) 16, 215 (2016)
16. Bhargava, B., Ranchal, R., Ben Othmane, L.: Secure information sharing in digital supply chains. In: Kalra, B.M. (ed.) 2013 3rd IEEE International Advance Computing Conference (IACC). 22 - 23 Feb. 2013, Ghaziabad, India, pp. 1636–1640. IEEE, Piscataway, NJ (2013)

https://doi.org/10.30844/wi_2020_d1-zeiringer

17. Arnold, V., Benford, T., Hampton, C., Sutton, S.G.: Competing pressures of risk and absorptive capacity potential on commitment and information sharing in global supply chains. European Journal of Information Systems 19, 134–152 (2010)
18. Vyatkin, V.: Software Engineering in Industrial Automation: State-of-the-Art Review. IEEE Trans. Ind. Inf. 9, 1234–1249 (2013)
19. Tran, T.H., Dobrovnik, M., Kummer, S.: Supply chain risk assessment: a content analysis-based literature review. IJLSM 31, 562 (2018)
20. Ho, W., Zheng, T., Yildiz, H., Talluri, S.: Supply chain risk management: a literature review. International Journal of Production Research 53, 5031–5069 (2015)
21. Fan, Y., Stevenson, M.: A review of supply chain risk management: definition, theory, and research agenda. Int Jnl Phys Dist & Log Manage 48, 205–230 (2018)
22. Ogulin, R., Selen, W., Ashayeri, J.: Determinants of informal coordination in networked supply chains. Journal of Ent Info Management 25, 328–348 (2012)
23. Lavastre, O., Gunasekaran, A., Spalanzani, A.: Supply chain risk management in French companies. Decision Support Systems 52, 828–838 (2012)
24. Colicchia, C., Creazza, A., Menachof, D.A.: Managing cyber and information risks in supply chains: insights from an exploratory analysis. Supp Chain Mnagmnt 24, 215–240 (2019)
25. Trkman, P., Desouza, K.C.: Knowledge risks in organizational networks: An exploratory framework. The Journal of Strategic Information Systems 21, 1–17 (2012)
26. Jarvenpaa, S.L., Majchrzak, A.: Interactive Self-Regulatory Theory for Sharing and Protecting in Interorganizational Collaborations. AMR 41, 9–27 (2016)
27. Bloodgood, J.M., Salisbury, W.D.: Understanding the influence of organizational change strategies on information technology and knowledge management strategies. Decision Support Systems 31, 55–69 (2001)
28. Manhart, M., Thalmann, S.: Protecting organizational knowledge: a structured literature review. J of Knowledge Management 19, 190–211 (2015)
29. Durst, S., Zieba, M.: Mapping knowledge risks: towards a better understanding of knowledge management. Knowledge Management Research & Practice 17, 1–13 (2019)
30. Mayring, P.: Einführung in die qualitative Sozialforschung. Eine Anleitung zu qualitativem Denken. Beltz Verlag, Weinheim, Basel (2002)
31. Wiengarten, F., Humphreys, P., Gimenez, C., McIvor, R.: Risk, risk management practices, and the success of supply chain integration. International Journal of Production Economics 171, 361–370 (2016)
32. Esmaeilian, B., Behdad, S., Wang, B.: The evolution and future of manufacturing: A review. Journal of Manufacturing Systems 39, 79–100 (2016)
33. Soares, M.N., Kauffman, M.E.: Industry 4.0: Horizontal Integration and Intellectual Property Law Strategies In England. OJ 16, 268 (2018)
34. Colicchia, C., Creazza, A., Noè, C., Strozzi, F.: Information sharing in supply chains: a review of risks and opportunities using the systematic literature network analysis (SLNA). Supp Chain Mnagmnt 24, 5–21 (2019)
35. Ulhaq, I., Kuruvilla, K.T., Nkhoma, M., Vu, H.H., Tuyet, N.T.: INFORMATION SECURITY RISKS IN SUPPLY CHAIN MANAGEMENT. IJISE 4, 58–68 (2016)

https://doi.org/10.30844/wi_2020_d1-zeiringer

36. Huong Tran, T.T., Childerhouse, P., Deakins, E.: Supply chain information sharing: challenges and risk mitigation strategies. Jnl of Manu Tech Mnagmnt 27, 1102–1126 (2016)
37. Alawamleh, M., Popplewell, K.: Risk in collaborative networks: relationships analysis. IJSOM 12, 431 (2012)
38. Aloini, D., Dulmin, R., Mininno, V., Ponticelli, S.: Supply chain management: a review of implementation risks in the construction industry. Business Process Mgmt Journal 18, 735–761 (2012)
39. Manzouri: A MODEL FOR SECURING SHARING INFORMATION ACROSS THE SUPPLY CHAIN. American Journal of Applied Sciences 10, 253–258 (2013)
40. Lotfi, Z., Mukhtar, M., Sahran, S., Zadeh, A.T.: Information Sharing in Supply Chain Management. Procedia Technology 11, 298–304 (2013)
41. Zeng, Y., Wang, L., Deng, X., Cao, X., Khundker, N.: Secure collaboration in global design and supply chain environment: Problem analysis and literature review. Computers in Industry 63, 545–556 (2012)
42. Le, H.Q., Arch-int, S., Nguyen, H.X., Arch-int, N.: Association rule hiding in risk management for retail supply chain collaboration. Computers in Industry 64, 776–784 (2013)
43. Bahroun, M., Harbi, S.: Risk management in the modern retail supply chain: Lessons from a case study and literature review. In: International Conference on Industrial Engineering and Systems Management (IESM); Framinan (Hg.) 2015 – The road ahead, pp. 1161–1170
44. Friday, D., Ryan, S., Sridharan, R., Collins, D.: Collaborative risk management: a systematic literature review. Int Jnl Phys Dist & Log Manage 48, 231–253 (2018)
45. Rangel, D., Silene Alexandre Leite, M.: Survey of supply chains risk assessment approaches. IIE Annual Conference and Expo, Pages 2128-2137 (2015)
46. Rangel, D.A., Oliveira, T.K. de, Leite, M.S.A.: Supply chain risk classification: discussion and proposal. International Journal of Production Research 53, 6868–6887 (2015)
47. Solomon, A.O., Ketikidis, P.H., Choudhary, A.: A Proposed Supply Chain Risk Management Framework. SSRN Journal (2011)
48. Biswas, S., Sen, J.: A Proposed Architecture for Big Data Driven Supply Chain Analytics. SSRN Journal (2016)
49. Thiel, C., Thiel, C.: Hare and Tortoise. Datenschutz und Datensicherheit 39, 663–667 (2015)
50. Birkel, H.S., Hartmann, E.: Impact of IoT challenges and risks for SCM. Supp Chain Mnagmnt 24, 39–61 (2019)
51. Situm, M., Mateos, R.M.M.: The strategic view of supply chain management and its association with risk. IJISM 11, 87 (2017)
52. Elliott, K., Patacconi, A., Swierzbinski, J., Williams, J.: Knowledge Protection in Firms: A Conceptual Framework and Evidence from HP Labs. European Management Review 16, 179–193 (2019)
53. Solomon, A., Ketikidis, P., Choudhary, A., Tiwari, M.: A Knowledge Based Decision Support System for Supply Chain Risk Management. Proceedings of European Decision Sciences Institute Conference EDSI (2012)
54. Salamai, A., Hussain, O.K., Saberi, M., Chang, E., Hussain, F.K.: Highlighting the Importance of Considering the Impacts of Both External and Internal Risk Factors on

https://doi.org/10.30844/wi_2020_d1-zeiringer

Operational Parameters to Improve Supply Chain Risk Management. IEEE Access 7, 49297–49315 (2019)
55. Xue, L., Cheng, Z., Hong, L., Zhao, X.: Risk-Mitigation in Supply Chain Digitization: A Study of System Modularity and IT Governance. SSRN Journal (2013)
56. Soares, M.N., Kauffman, M.E.: INTELLECTUAL PROPERTY LAW IN THE FOURTH INDUSTRIAL REVOLUTION: TRADE SECRETS RISKS AND OPPORTUNITIES. Revista Jurídica 52, 199–224 (2018)
57. Sofka, W., Shehu, E., Faria, P. de: Multinational subsidiary knowledge protection—Do mandates and clusters matter? Research Policy 43, 1320–1333 (2014)
58. Thalmann, S. and Ilvonnen, I.: Why should we investigate knowledge risks incidents? - Lessons from four cases. Proceedings of 53rd Hawaii International Conference on System Sciences (2020)
59. Subramani, P., Agarwal, R.: Opportunities and pitfalls associated with coordination structures in supply chain management: An exploratory case study. International Journal of Supply Chain Management 2, Pages 17-31 (2013)

https://doi.org/10.30844/wi_2020_d1-zeiringer

Appendix

Domain	Knowledge Management	Operations Management	Information Systems	Further Areas
Journal/Conference	*VINE: The journal of information and knowledge management systems, Knowledge Management Research & Practice, Journal of Knowledge Management, Proceedings of the Conference Professional Knowledge Management*	*Supply Chain Management: An International Journal, International Journal of Production Research, International Journal of Production Economics, Journal of Purchasing and Supply Management, International Journal of Physical Distribution & Logistics Management, International Journal of Services and Operations Management, International Journal of Supply Chain Management, International Journal of Logistics Systems and Management, The International Journal of Logistics Management, 20th International Working Seminar on Production Economics, International Journal of Operations & Production Management, International Journal of Integrated Supply Management, Journal of Manufacturing Technology Management, International Journal of Production Research, Production Planning & Control, IIE Annual Conference and Expo, International Conference on Industrial Engineering*	*International Journal of Information Systems and Engineering, Computers in Industry, European Journal of Information Systems*	*Academy of Management Review, International Journal of Management and Decision Making, China-USA Business Review, Journal of Advances in Management Research, Decision Support Systems, Direccion y Organización, Journal of Enterprise Information Management, Business Process Management Journal, International Journal of Innovation Management, Design, Automation & Test in Europe Conference & Exhibition, Proceedings of European Decision Sciences Institute Conference EDSI, International Journal of Applied Engineering Research, IEEE International Conference, AIP Conference Proceedings 2097, IEEE Access, Procedia Technology, American Journal of Applied Sciences, Revista Opinião Jurídica, SSRN Journal, Research Policy, Datenschutz und Datensicherheit*
Keywords (primary & secondary)				
knowledge protection/risk (management)	3	17	2	7
(data-centric) collaboration	2	4	1	4
data exchange /sharing	2	1	1	5
industry 4.0		3		4
supply chain (management)	1	21	4	15
strategic management	1			1
digitalization		1		1
competitive knowledge	1			
interorganisational (knowledge transfer)	2		1	
protection capabilities /practices	1			1
security/privacy			1	4
Total	13	47	10	42

Appendix 1.Review Matrix, categorized in domains

https://doi.org/10.30844/wi_2020_d1-zeiringer