Received 18 April 2019
Revised 13 November 2019
13 February 2020
Accepted 20 March 2020

Information technology and risk management in supply chains

Diana Fischer-Preßler and Kathrin Eismann
Department of Information Systems and Social Networks, University of Bamberg, Bamberg, Germany
Rafael Pietrowski
Department of Information Systems and Information Management, University of Cologne, Cologne, Germany
Kai Fischbach
Department of Information Systems and Social Networks, University of Bamberg, Bamberg, Germany, and
Detlef Schoder
Department of Information Systems and Information Management, University of Cologne, Cologne, Germany

Abstract

Purpose – This paper reviews and classifies research connecting supply chain risk management (SCRM) and information technology (IT) and derives a structured proposal for fruitful research directions.

Design/methodology/approach – The authors conducted a systematic literature review of the interplay of SCRM and IT, drawing from major journals in the relevant fields. These findings are enriched by experiences from a three-year international research project.

Findings – Current research focuses on the role of IT for risk reduction, rather than for risk identification, analysis and monitoring. While much research has investigated operational supply chain risk, fewer insights into disruption risk are available. There is little research on the role of IT in SCRM beyond its potential to enhance information sharing among supply chain partners. To address these gaps, the paper proposes a two-dimensional framework to categorize IT potential for SCRM according to the source and impact of disruption risk on physical supply chain flows, which suggests promising directions for future research.

Originality/value – The paper offers a systematic review to further our understanding of the relationship of SCRM and IT. In addition, it presents and discusses nine areas for further research aimed at mitigating the gaps identified at the intersection of SCRM and IT.

Keywords Supply chain management, Supply chain risk management, Risk management, Information technology, Information systems, Literature review

Paper type Literature review

Introduction

Modern supply chains are highly complex, with many parallel physical and information flows ensuring that products are delivered to the right place at the right time in the right quantities and in a cost-effective way. Competitive pressure and globalization of markets within almost all industries compel organizations to strive for increasingly extensive and efficient intra- and interfirm supply chains that can operate throughout the world, which makes these supply chains more and more vulnerable to risks (Manuj and Mentzer, 2008). These risks stem from the focus on efficiency rather than effectiveness, growing uncertainties in demand and supply, outsourcing and offshoring in low-cost countries, the globalization of markets and decreased product and technology life cycles (Wagner and Neshat, 2010). Moreover, many areas of supply chain operations, ranging from the interorganizational management of information to the distribution of physical assets, are potentially affected by threats from inside the supply chain, such as cybersecurity breaches, document forgery and counterfeiting (Urciuoli and Hintsa, 2016).

International Journal of Physical Distribution & Logistics Management
Vol. 50 No. 2, 2020
pp. 233-254

0960-0035
DOI 10.1108/IJPDLM-04-2019-0119

In addition, human-made and natural disasters that adversely affect societies throughout the world are disruptive events for supply chains, with far-reaching impacts. For example, the 9/11 terrorist attacks in New York City and at the Pentagon caused serious transportation difficulties for manufacturers when the government closed borders, shut down all air traffic and evacuated buildings throughout the United States in response (Sheffi, 2001). Hurricanes striking the US Gulf Coast region have caused instability in oil supplies and prices because of damages to petroleum-refining and transportation infrastructures (Knemeyer *et al.*, 2009). Such major occurrences, as well as other less deadly, but nevertheless economically impactful incidents, have also disrupted many companies' ability to run their businesses (Chopra and Sodhi, 2004).

It can be complex and difficult to identify and assess likely risk sources and their impacts on supply chain operations. Firms must consider not only the direct risk to their own operations, but also the risk to all other supply chain partners as well as risk caused by the linkages between these organizations (Knemeyer *et al.*, 2009). Companies often invest in information technology (IT) to handle such risk better (Sambhara *et al.*, 2016). In the past 10–15 years, these investments have increasingly expanded beyond more established IT solutions such as enterprise resource planning (ERP) systems to include novel applications such as advanced analytics and business intelligence tools, cloud computing and mobile applications (Luftman *et al.*, 2015). Over roughly the same period, social media such as wikis and (enterprise) social networks have gained importance for managing organizational assets (Leonardi *et al.*, 2013).

There is a relatively large body of literature relating to the functionalities of IT in supply chain risk management (SCRM). Colicchia *et al.* (2018b), for instance, summarize research activities related to risks that arise from disruption, as well as the opportunities to reduce risks by sharing information among supply chain partners. In addition, there have been frequent investigations of IT developments that support the traceability of goods along the supply chain (Ringsberg, 2014). However, many of the relevant publications on the role of IT in supply chain management (SCM) have precluded adopting a risk perspective (e.g. Varma and Khan, 2014) or have considered SCRM without a focus on IT (e.g. Vanany *et al.*, 2010). Papers that have explored the benefits of IT for SCRM in specific cases and scenarios (e.g. Day *et al.*, 2009; Meijboom *et al.*, 2011) do not provide comprehensive insights into state-of-the-art uses of IT in different risk settings.

Nevertheless, the increasing vulnerability of modern supply chains to risks that arise from regular supply chain operations as well as disruptive events demonstrates the importance of research into how IT might contribute to managing those risks. In this paper, we first provide a comprehensive survey of research on the interplay between SCRM and IT as well as a clear and consistent framework for analyzing IT in SCRM. We then present a structured proposal for future research directions based on the review findings and enriched by insights from discussions with practitioners participating in a three-year international research project. In particular, we:

(1) clarify the extent to which the literature has produced scientific insights into the interplay between SCRM and IT;

(2) review and classify papers focused on IT usage for SCRM according to their approach and lens on supply chain risk and IT; and

(3) explore trends in SCRM and IT and suggest promising areas for future research.

The remainder of this paper is organized as follows. The background section introduces SCRM and IT. We then explain the systematic literature review methodology. The section that follows presents the results and discusses their implications for research at the intersection of SCRM and IT. Based on these insights, we introduce a research framework that addresses the research gaps we uncovered and identifies opportunities for future research. In addition, we provide practitioners' insights into pressing SCRM issues that could benefit from advanced IT applications to handle risks. We summarize our findings in the conclusion.

Conceptual background

Supply chain management and risk sources

Supply chain risks are the impact and probability of the occurrence of an incident in the information, material or product flow from all suppliers to the end users of a supply chain that endangers the achievement of supply chain goals (Jüttner *et al.*, 2003). While risk is often used interchangeably with uncertainty (i.e. insufficient information to identify all potential outcomes), researchers have argued that, in contrast to uncertainty, risk is associated exclusively with negative impacts on the supply chain (Wagner and Bode, 2008). For instance, the risk associated with natural disasters can only affect the supply chain negatively, whereas the uncertainty in demand can also exceed expectations (Simangunsong *et al.*, 2012). Thus, risk goes beyond the concept of uncertainty by focusing on the negative impacts of events and circumstances that can adversely affect supply chain operations and outcomes.

SCRM is the management of risk in a supply chain (Norrman and Jansson, 2004). The interconnectedness of modern supply chains can create a ripple effect – that is, a supply chain disturbance at one point in the supply chain can affect all partners in that supply chain (Shi, 2004). Supply chain risk thus inevitably extends beyond the boundaries of any single organization, and any approach to risk management from a supply chain perspective must, therefore, have a broader scope than that of a single organization and take into account insights regarding how key processes are executed across the organizations involved (Jüttner *et al.*, 2003).

Risk in the supply chain literature has typically been classified into two broad risk types (Ho *et al.*, 2015), although different researchers use different terminology in drawing the distinction: internal and external (Jüttner *et al.*, 2003); micro-level and macro-level (Ho *et al.*, 2015); and operational and disruption (Tang, 2006). We adopt the Tang (2006) terminology because the broad classification of operational and disruption risk provides categories for synthesizing the different sources and consequences of risk while also leaving some leeway for subcategories that may emerge from the literature.

Operational risk exists intrinsically in all supply chains and often arises as a result of their management and structures, such as uncertain supplies, costs and customer demands. Disruption risk refers to external disruptive events caused by humans or nature, such as terrorist attacks, wars, floods and earthquakes, but also economic crises such as currency fluctuations or labor strikes (Tang, 2006). In contrast to operational risk, disruption risk cannot be generally prevented by the specific organizations within the supply chain, but nevertheless can be addressed by SCRM approaches, such as through enhanced contingency planning or resilience capabilities.

Information technology and supply chain risk management

Hardware and software such as electronic data interchange (EDI), radio frequency identification (RFID) technology, bar codes, the Internet and information systems such as electronic commerce systems, cloud computing, proprietary applications, ERP and manufacturing systems are all examples of IT frequently found in an SCM context (Gunasekaran *et al.*, 2006; Varma and Khan, 2014). These have generally been considered important resources in SCM (Varma and Khan, 2014).

To investigate in detail how IT can support SCRM in our study, we apply the integrated IT risk management framework proposed by Bandyopadhyay *et al.* (1999), which provides a comprehensive perspective on and includes classic tasks of risk management in supply chains (Trkman and McCormack, 2009). *Risk identification* is the process of determining the potential impact of threats to the supply chain (Bandyopadhyay *et al.*, 1999); IT can, for instance, contribute to supply chain risk identification through visual supply chain mapping, which is an approach for visualizing the upstream and downstream flow of goods, information and money from suppliers to customers (Tummala and Schoenherr, 2008). *Risk analysis* comprises approaches for understanding and exploring the extent of losses that result when threats detected as potential in the risk identification stage actually come to pass (Bandyopadhyay *et al.*, 1999); IT can provide enhanced data-analytical and modeling techniques to aid the decision-making process and risk analysis (Varma and Khan, 2014). *Risk reduction* is the implementation of measures to reduce risk and thus ensure the supply chain's best possible protection from threats (Bandyopadhyay *et al.*, 1999); by enhancing data acquisition, traceability and recording of flows within the supply chain, IT can facilitate intervention in case of harm or damage and thus support the reduction of risk within the supply chain (Chow *et al.*, 2007). *Risk monitoring* serves to evaluate the performance of risk-reducing measures and provides a continuous audit function (Bandyopadhyay *et al.*, 1999); IT can help in this respect, for instance, by providing a catalog of identified risk factors, consequence severity levels, risk probabilities and supply chain risk triggers (Varma and Khan, 2014).

Methodology

We conducted a *scoping review* to evaluate the extent to which prior research provides insights into the role of IT to support risk management along supply chains (Paré *et al.*, 2015). Following Paré *et al.* (2016), the procedure we used to identify and analyze relevant publications comprises four steps: literature search, literature selection, data extraction and data analysis.

In the *literature search*, we aimed at comprehensive coverage of relevant publications that investigate applications and use of IT in the SCRM context. Our focus was on research articles published in leading journals whose contents relate to SCM, logistics, management science, operations research or information systems, as we expected major contributions are made in such outlets (Webster and Watson, 2002). We included publications from a set of scientific journals listed in the top category of at least one of the following: VHB-JOURQUAL3 2015 Journal Ranking (Verband der Hochschullehrer für Betriebswirtschaft, 2015), Erasmus Research Institute of Management, 2016 Journal List (Erasmus Research Institute of Management, 2016) and ABDC Journal Quality List 2016 (Australian Business Deans Council, 2016). By combining these rankings, we intended to support geographic diversity and maximize the representativeness of results. Furthermore, we included publications from 11 SCM journals that received grades of 1 or greater in the 2015 impact factor ratings. Overall, we considered 39 scientific journals as the basis for our literature search.

We conducted a keyword-based search in the titles, abstracts and keywords of the relevant journals through indexing databases, primarily Business Source Ultimate, Emerald Insight and ScienceDirect. Our review focused on outcomes and applications from research at the intersection of SCRM and IT. From this conceptualization of the topic, we derived the search terms for the literature search, which we intentionally kept broad to avoid excluding potentially relevant studies. Given our research focus, we included "supply chain" as a relevant keyword. We did not include synonyms of this concept for practical reasons and because preliminary searches had revealed that many papers with SCM-related content used this term at least in addition to others, such as logistics or warehouse management. For the risk dimension, we considered multiple synonymous and related terms to find as many potentially relevant papers as possible (Ghadge *et al.*, 2012). For the IT dimension, we searched for the term "information," as preliminary searches revealed that articles often did not refer to the specific terms "information technology" or "information systems" for IT-related aspects.

The final search phrase was: *supply chain AND information AND (risk OR vulnerability OR resilience OR security OR safety OR disruption OR crisis OR emergency OR disaster OR incident OR accident)*. We restricted the search to the last 15 years, including all articles published between 2004 and 2018, a timespan that captures a period during which developments in information and communications technology (advanced business intelligence, analytics solutions and social media, most prominently) opened up new possibilities for IT to support managerial activities at the same time that highly globalized and optimized supply chains became increasingly exposed to risks. Overall, the literature search yielded 406 articles that met our search criteria.

Our *literature selection* process had two of this paper's authors read the titles and abstracts of all 406 articles. If both seemed relevant to the focus of the review, they screened the complete articles to make a final decision. Two selection criteria were applied simultaneously: we included only articles that covered both SCRM and IT, our research areas of interest; and we excluded all publications that had not been subject to peer review, such as prefaces, book reviews and interviews. Following Paré *et al.* (2015), we included both empirical and conceptual research articles. Initially, the two authors independently assessed whether an article was relevant. When the independent screening resulted in different judgments, they worked toward agreement by discussing together their reasons for including or excluding a study. After eliminating irrelevant items, we obtained 55 articles. The interrater reliability, pertaining to the overall inclusion decision, was $\varkappa = 0.63$.

For *data extraction* and *data analysis* with these 55 articles, we followed the recommendations of Bandara *et al.* (2015) for qualitative deductive content analyses. Codes were established *a priori* based on the risk dimension, which is categorized into operational and disruption risk (Tang, 2006), and the IT dimension, which consists of IT functionalities, applications and uses for risk identification, risk analysis, risk reduction and risk monitoring (Bandyopadhyay *et al.*, 1999). One author initially assigned the findings of each of the reviewed articles to one or more categories on both dimensions and gathered further information from each study regarding the study type (i.e. empirical, conceptual or literature review), the type of supply chain investigated, sources of risk addressed and IT applications, functionalities and/or uses mentioned (open categories). A second author then reviewed, complemented and revised these categorizations. The outcome of the data extraction stage is a concept matrix in which each article is assigned to one or more salient concepts (Webster and Watson, 2002).

In addition to the systematic literature review, we sought practical guidance on further research perspectives by discussing our insights with senior employees and supply chain experts from German companies (e.g. REWE Group, SAP, Küehne + Nagel) that participated in a three-year international research project funded by the German Federal Ministry of Education and Research.

Results of the systematic literature review

Supply chain risk

We summarize and discuss further the results of the literature analysis, beginning with an analysis of supply chain risks covered by the literature. As Table 1 shows, 34 of the 55 papers investigate operational risk, whereas only 11 refer to disruption risks. An additional ten papers did not commit to one or more specific sources of risk or refer explicitly to more than one risk type. There is no temporal trend in the respective share of risk types; in fact, studies of operational risks outnumber those on disruption risks for almost all the years covered by our review.

Research has most frequently investigated supply chains whose outcomes are intended to address risks themselves. For operational risk, healthcare supply chains in the public or private sector are most frequently investigated, whereas for disruption risk, the largest number of papers relates to humanitarian or disaster relief supply chains, as Table 2 indicates. In health-related supply chains, hospitals and other healthcare providers face increasing efficiency pressures that necessitate they manage their assets and resources at reduced costs while maintaining high standards of service. In response to this demand, research has, in particular, treated transitions between different service providers (e.g. of patients, drugs or medical products) as potential sources of risk to patients' treatment or physical safety (e.g. Ford and Hughes, 2007; Gonul Kochan *et al.*, 2018).

In contrast, humanitarian and disaster relief agencies from both the public and private sectors typically address resource allocation problems, especially in the aftermath of natural disasters such as hurricanes. Research suggests that such operations are likely to suffer from insufficient SCM capabilities (which would be developed through training staff, educating vulnerable populations, creating organizational response plans and interorganizational coordination, and in other ways; Kunz *et al.*, 2014); these can increase the degree of harm and damage (Gatignon *et al.*, 2010).

Supply chains in the food-processing industries and, in this context, the safety of foods delivered for consumption (e.g. Taylor and Fearne, 2006) are another focus of research activity. In addition, several papers investigate supply chain risk reduction in the manufacturing sector (e.g. Yang *et al.*, 2009), as well as in the apparel and electronics industries (e.g. Machado *et al.*, 2018). These supply chains have in common that they involve physical goods or services that, should they become unavailable or damaged, could not only harm supply chain partners but also affect customers. Finally, a large number of papers, primarily covering operational risk sources, are unspecific as to the fields of application to which they refer or rely on data from different areas of operation.

All the reviewed papers that investigate operational risks discuss hazards that arise from uncertainties inherent in the supply chains themselves (e.g. regarding the availability, locations and qualities of goods or services). This holds true especially for agri-food supply chains, in which traceability, for instance, is related to product quality and the risk of deterioration (Aiello *et al.*, 2015). In other industrial contexts such as electronics, risk can emerge from a lack of visibility of operations along the supply chain, which Coronado Mondragon *et al.* (2009) attribute to technical communication shortcomings, such as insufficient network reliability and connectivity. Similarly, Raisinghani and Meade (2005) reference the visibility, velocity and flexibility of operations as factors that can increase supply chain resilience in mobile communications industries, and Deshpande *et al.* (2006) identify increased inventory costs, unanticipated demand needs and poorly coordinated goods and processes as potential sources of operational risk within the US Coast Guard.

Aligning processes as well as product and information flows within and across organizations is generally expected not only to enhance supply chain efficiency but also to

Supply chain risk type	Number of articles
Operational risk	34
Disruption risk	11
Unspecific/both	10
Overall	55

Table 1.
Article categorization - supply chain risk

		Number of articles					
	Overall	Operational risk		Disruption risk		Unspecific/both	
Humanitarian/ disaster relief	7	1	Yang *et al.*, (2009)	6	Charles *et al.*, (2016); Chen *et al.*, (2008); Day *et al.*, (2009); Gatignon *et al.*, (2010); Gupta *et al.*, (2016); Maon *et al.*, (2009)	0	
Health care	6	5	Ford and Hughes (2007); Gonul Kochan *et al.*, 2018; Meijboom *et al.*, (2011); Riley *et al.*, (2016); Xie *et al.*, (2016)	1	Gopalakrishna-Remani *et al.*, (2018)	0	
Manufacturing	5	0		1	Giannakis und Louis (2011)	4	Brandon-Jones *et al.*, (2014); Fan *et al.*, (2017); Lee *et al.*, (2011); Yang *et al.*, (2009)
Food-related	4	3	Aiello *et al.*, (2015); Scholten und Schilder (2015); Taylor und Fearne (2006)	0		1	Ringsberg (2014)
Apparel	3	2	d'Aubeterre *et al.*, (2008); Machado *et al.*, (2018)	1	Pettit *et al.*, (2010)	0	
Electronics	3	2	Blackman *et al.*, (2013); Kembro *et al.*, (2017)	0		1	Basole und Bellamy (2014)
Logistics	2	2	Klein und Rai (2009); Mei und Dinwoodie (2005)	0		0	
Retail	2	2	Richey und Autry (2009); Jiang *et al.*, (2017)	0		0	
Multiple/ unspecific	23	17	e.g. Chow *et al.*, (2007); Coronado Mondragon *et al.*, (2009); Jede and Teuteberg (2016); Lavastre *et al.*, (2012); Pibernik *et al.*, (2011)	2	Hall *et al.*, (2012); Skipper und Hanna (2009)	4	Chae (2015); Levermore *et al.*, (2010); Urciuoli und Hintsa (2016); Colicchia *et al.*, (2018b)

Table 2.
Article categorization - supply chain context

reduce risk that stems from a lack of coordination and control (Power, 2005). In particular, improved information sharing and increased accessibility of timely and relevant information can support SCRM through enhanced traceability and visibility of goods and activities along the entire supply chain. Prior research has paid specific attention to the integration of information flows to reduce operational risk. Making strategic and tactical information available to supply chain partners is not only positively associated with supply chain performance but can also support SCRM activities, for instance, by allowing enhanced demand and production planning and thus reducing the bullwhip effect (Klein and Rai, 2009).

Research also emphasizes that IT itself constitutes a major risk factor in increasingly interwoven supply chains. IT risks include, among others, cyber and information security risks, the exploitation of a supply chain partner's strategic information (Colicchia *et al.*, 2018a), IT infrastructure breakdowns, the lack of effective systems integration and the incompatibility of IT platforms (Yang *et al.*, 2012). Hence, although IT is meant to improve performance and security within a supply chain, it also introduces new risks and dependencies.

With respect to disruption risk, the management of supply chains that address the effects of disaster events is a prominent research theme. Humanitarian organizations, constrained by limited resources and often dependent on donations, must respond to as many needs as possible as quickly as possible. At the same time, high levels of uncertainty, limited budgets and cost efficiency pressures can run counter to organizations' efforts (Gatignon *et al.*, 2010). Many problems arise especially from insufficiencies in collecting, processing and sharing event-related information. In that sense, issues that arise in humanitarian and disaster relief supply chains are not dissimilar to those addressed in the context of operational risk. Day *et al.* (2009), for instance, address specific information flow impediments in disaster relief supply chains, such as the inaccessibility of data and inconsistency of data and information formats. Research has addressed this problem area by developing common data standards (Chen *et al.*, 2008) and methods for overcoming issues of delayed reporting and lead time variation (Gopalakrishna-Remani *et al.*, 2018), among other approaches.

New supply chains often must be formed to respond to a triggering event, or existing ones at least adapted – raising another challenge for operators of humanitarian and disaster relief supply chains. Day *et al.* (2009) note that unlike with industrial supply chains, the responsiveness of disaster relief supply chains is crucial, even under conditions of extreme uncertainty and short life cycles, which makes it challenging to establish effective information flows. When in response to an emerging event organizations need to form new networks with limited time to formalize processes and foreseeable termination of joint efforts, it is unlikely they can rely upon established relationships to respond to an emerging event. In addition, despite the typically strong commitment of humanitarian agencies, a comprehensive knowledge base is often missing, and they may have issues prioritizing SCM activities. The short-term nature of disaster supply chains and insufficient funding hinder the adoption of strategic posture and technologies. Failure to coordinate the many decentralized agencies and large numbers of volunteers is a recurring criticism (Maon *et al.*, 2009). Moreover, experiences gained responding to one event cannot necessarily be transferred to other disaster supply chain operations, as different types of events may require different supply chain designs (Charles *et al.*, 2016).

Applications and use of information technology to support supply chain risk management

Considering what prior research reveals about the role of IT to manage both operational and disruption supply chain risk, we find that the vast majority of relevant studies addresses the reduction of risk. As is evident from Table 3, 52 of the 55 articles analyzed relate to risk reduction, while only ten include insights into risk identification and analysis and eight relate to risk monitoring. Twelve papers were assigned to more than one category; typically, these works pursued a comprehensive contingency planning or resilience approach in which risks were supposed to be addressed through SCM integration and information sharing across different risk management tasks. Patterns are similar for research on both operational and disruption risk.

Most of the articles that were assigned to only one risk management category refer exclusively to the potential of IT to reduce risks. Strikingly, almost all these works broach issues of supply chain integration and information sharing, often in terms of the strategic

Table 3. Article categorization - supply chain risk management (articles were assigned to more than one category)

	Number of articles Risk identification		Risk analysis		Risk reduction		Risk monitoring	
Operational risk	4	Lavastre *et al.*, (2012); Riley *et al.*, (2016); Varma und Khan (2017); Yang *et al.*, (2012)	2	Lavastre *et al.*, (2012); Yang *et al.*, (2012)	33	e.g. Aiello *et al.*, (2015); Ford und Hughes (2007); Jede und Teuteberg (2016); Jiang *et al.*, (2017); Meijboom *et al.*, (2011)	2	Lavastre *et al.*, (2012); Yang *et al.*, (2012)
Disruption risk	4	Giannakis und Louis (2011); Gupta *et al.*, (2016); Hall *et al.*, (2012); Pettit *et al.*, (2010)	6	Chen *et al.*, (2008); Giannakis und Louis (2011); Gupta *et al.*, (2016); Hall *et al.*, (2012); Pettit *et al.*, (2010); Skipper und Hanna (2009)	10	e.g. Charles *et al.*, (2016); Day *et al.*, (2009); Gatignon *et al.*, (2010); Hall *et al.*, (2012); Maon *et al.*, (2009)	4	Chen *et al.*, (2008); Giannakis und Louis (2011); Pettit *et al.*, (2010); Skipper und Hanna (2009)
Unspecific/ both	2	Chae (2015); Fan *et al.*, (2017)	2	Basole und Bellamy (2014); Fan *et al.*, (2017)	9	e.g. Brandon-Jones *et al.*, (2014); Lee *et al.*, (2011); Ringsberg (2014); Urciuoli und Hintsa (2016); Yang *et al.*, (2009)	2	Chae (2015); Fan *et al.*, (2017)
Overall	10		10		52		8	

thrust of supply chain partners (e.g. Blackman *et al.*, 2013). The evident role ascribed to IT in these papers is to help reduce uncertainty through information sharing and collaboration. The literature has investigated not only "soft" organizational factors such as employee training (Riley *et al.*, 2016) and willingness to share information (Fawcett *et al.*, 2007) but also the positive effect of interorganizational IT use on organizational collaboration, which in turn can support contingency planning effectiveness (Hall *et al.*, 2012). Following from Olorunniwo and Li (2010), it is the operational attributes of IT that can increase supply chain performance, particularly the improvements they offer for communications, storing information and increasing information visibility along the supply chain.

Although much prior research mentions IT only in a very broad sense, referring to its general capability to support supply chain integration, information sharing and collaboration, the potential of several specific IT solutions to enhance supply chain performance and identify, analyze, reduce and monitor operational and disruption risks has already been investigated. For instance, research stresses the potential of IT applications such as ERP systems, warehouse and transportation management systems and database management and mining solutions to support information supply chains (Varma and Khan, 2014). Most prominently, IT enables supply chain partners to access previously unavailable information about, for instance, warehouse operations (Kembro *et al.*, 2017) and vendor fraud (Varma and Khan, 2017), and to set up efficient information supply chains through integrated databases and information systems (Deshpande *et al.*, 2006). Table 4 provides an overview of IT functionalities and applications discussed in the literature.

Table 4.
Article categorization - IT functionalities (articles were assigned according to their main contribution)

IT functionalities and applications	Number of articles	Existing research themes (examples)
Overall IT strategy and IT unspecific with respect to certain tools and applications to support information sharing and collaboration	26	(1) IT can support efficient structures of interorganizational information sharing and collaboration, which increases supply chain resilience (Brandon-Jones *et al.*, 2014) and the efficiency of response to disruptive events (Gatignon *et al.*, 2010) and facilitates planning for potential occurrences (Skipper und Hanna, 2009) (2) Strategic investments in IT are useful to foster interfirm collaboration and reduce (operational) supply chain risk (e.g. Lavastre *et al.*, 2012) (3) Issues related to the implementation of integrated information and communications technologies to facilitate interorganizational coordination reduce the likelihood of unexpected disruptions (Maon *et al.*, 2009) and support early identification and analysis of potential disruption risk sources (Hall *et al.*, 2012)
IT tools and applications to support visibility and traceability	8	(1) RFID increases the visibility and traceability of goods along the supply chain, which reduces risk that emerges from a lack of efficiency, accuracy and security of material and information flows (e.g. Aiello *et al.*, 2015; Cannon *et al.*, 2008) (2) Wireless communications can speed up information flows and help with tracking supply chain goods (Coronado Mondragon *et al.*, 2009) (3) Video technologies provide real-time information about warehousing operations (Kembro *et al.*, 2017) (4) Network analysis and information visualization support the understanding of complex supply network dependencies, which helps in identifying and analyzing potential risks (Basole und Bellamy, 2014) (5) Monitoring conversations on Twitter with social media analytics can help keep track of potential risk sources (Chae, 2015)
IT tools and applications to support information sharing and collaboration	7	(1) E-procurement solutions can support information sharing and collaboration along the supply chain (Puschmann und Alt, 2005) (2) Cloud computing and Web-based information exchanges enable fast and easy information sharing among supply chain partners, which can help reduce risks that arise from uncertainty regarding supply chain partners' operations (Gonul Kochan *et al.*, 2018; Chow *et al.*, 2007) (3) Electronic reporting systems can speed up reporting of risk and hence support efficient removal of risk sources (Gopalakrishna-Remani *et al.*, 2018; Mei und Dinwoodie, 2005)

(*continued*)

IT functionalities and applications	Number of articles	Existing research themes (examples)
Decision support systems	2	(1) IT allows efficient location selection and decisions on quantity of stock for disaster response supply chains (Charles *et al.*, 2016) (2) Multi-agent-based decision support can facilitate risk identification, assessment, implementation of risk management actions and optimization in complex environments (Giannakis und Louis, 2011)
IT adoption	3	(1) Factors that influence adoption of IT for SCRM, such as security concerns that can hinder investments in IT for SCRM (Lee *et al.*, 2011) or environmental forces that drive implementation (Xie *et al.*, 2016)
System design	6	(1) Integrated architectures for information gathering, database management and decision help increase situational awareness and facilitate identifying, monitoring, analyzing and eventually reducing risks that arise from a complex decision-making environment (e.g. Levermore *et al.*, 2010; Yang *et al.*, 2012) (2) Disaster IT should support a decentralized supply chain, as many organizations must be managed, comprise a social network component to enable communication during disruption events in which new relationships must be built, provide spatial information about affected areas, allow easy data upload and access for all involved, support different data formats, comprise timely reporting systems and be easy to use since users will be people with various backgrounds (Day *et al.*, 2009) (3) Adoption of shared data standards supports supply chain interoperability and facilitates analyzing, monitoring and reducing identified risks in response to major incidents (Chen *et al.*, 2008)
IT as a risk factor	2	(1) IT-supported information supply chains can suffer from intentional and unintentional information leakage (Colicchia *et al.*, 2018a) (2) Information management involves cybersecurity, document forgery and trust and verification risks (Urciuoli und Hintsa, 2016)

Table 4.

RFID, for instance, is mentioned repeatedly in the context of operational risk reduction, as it provides information about the state of goods at all times that can be made available to supply chain partners (Cannon *et al.*, 2008). Thus, RFID can reduce, for instance, the risk of loss or degradation in food supply chains (Aiello *et al.*, 2015). Similarly, ERP and e-procurement systems can help reduce risks by facilitating information sharing and collaboration (Puschmann and Alt, 2005). ERP systems can also enable entities along the supply chain to become aware of abnormalities, which can help identify and mitigate hazards such as vendor fraud (Varma and Khan, 2017). In line with existing findings on IT use in SCM more generally, research has considered dedicated decision-support systems that can also serve SCRM-related tasks (Giannakis and Louis, 2011).

Other forms of IT that have received attention are basically applications that complement existing solutions by providing access to novel and/or real-time information about operations, such as wireless networks (Coronado Mondragon *et al.*, 2009) and video technology (Kembro *et al.*, 2017) that can complement ERP, procurement and warehousing systems. Furthermore, data and information can be transmitted faster using novel channels of information sharing, such as cloud computing (Jede and Teuteberg, 2016) and Web-based communication (Chow *et al.*, 2007). Electronic reporting practices can reduce both operational and disruption risks by counteracting delays, reducing reporting error rates and ensuring prompt response to risk occurrences (Mei and Dinwoodie, 2005). Finally, research has elaborated on principles for secure information sharing and communication to reduce information-related risks (d'Aubeterre *et al.*, 2008), which can supplement currently used tools and practices.

Other research themes affect SCRM more indirectly, such as IT implementation and adoption (e.g. questions surrounding the adoption of IT for SCRM practices), system design (e.g. IT features that support SCRM in response to disasters and major emergencies) and IT as a risk factor as discussed earlier. Table 4 articulates these research themes in more detail.

Discussion of review results

In summary, we find that much of the research that has investigated the role of IT for SCRM in the past 15 years has addressed IT as a means to enable information sharing and collaboration. By and large, the role ascribed to IT in these studies is one of providing access to new or additional existing real-time sources of information, facilitating information sharing and exchange among different supply chain entities and especially decreasing operational risks by reducing uncertainty and facilitating prompt responses to emerging risk. While information sharing and integration of information supply chains can easily and more generally be related to the reduction of operational risk and uncertainty, many of these studies have concentrated on the role of IT to enhance supply chain performance. Only a few articles to date have related the collaborative capabilities of IT to specific aspects of SCRM, such as contingency planning (Skipper and Hanna, 2009) and supply chain resilience (Brandon-Jones *et al.*, 2014). Moreover, SCRM is more than just information management. Flows of physical products and materials are particularly subject to operational and disruption risk and hence those flows are relevant for SCRM. It follows that comprehensive approaches that analyze the use of IT across all stages of SCRM and that integrate the management of information as well as supply chain goods could provide valuable insights.

Our literature review also reveals that while many papers investigate operational supply chain risk, research on disruption risk is less common. Most of the studies that refer explicitly to disruption risks investigate only one risk source, namely disaster events, be they human-made or natural. Of these, only three provide evidence regarding the (IT-supported) management of supply chains exposed to low-probability, high-impact events such as disasters (namely Giannakis and Louis, 2011; Gopalakrishna-Remani *et al.*, 2018; Pettit *et al.*, 2010), while many of the others are unspecific in terms of the risk source and type. Thus, studies that address IT use for managing specific disruption risks in an industrial context beyond natural and human-made disaster events would clearly address a research gap. Furthermore, promising insights could also lie in research on disruptions such as labor disputes, riots, supplier bankruptcies that do not rise to the level of major disasters.

Most research to date has considered the role of IT in risk reduction, but rarely in risk identification, analysis or monitoring. This may be due to the current focus on cost, time and quality in supply chains. Overcompensating with respect to these areas of focus could counteract them and end up increasing the vulnerability of supply chains (Norrman and Jansson, 2004). For instance, risk may arise from dynamic relationships among supply chain partners and complex interdependencies that cause difficulties for risk identification and monitoring. Thus, the costs, willingness, dependencies and potential risks that exist for companies along the supply chain may complicate integrated SCRM. Furthermore, the absence of research on risk identification, analysis and monitoring might also result from the lack of a unified approach that links the information sharing, collaborative and other capabilities of IT to specific aspects of SCRM.

What is more, when it comes to IT for SCRM that goes beyond established applications such as RFID, ERP, EDI and warehousing systems (Varma and Khan, 2014), research is more fragmented in terms of concrete tools and applications. For decentralized and ad-hoc supply chains, such as those typical for humanitarian relief operations in the aftermath of a disaster or major incident, establishing design requirements for information systems and databases seems to have become a promising approach to facilitate interorganizational collaboration in particular (Yang *et al.*, 2009). As Deshpande *et al.* (2006) suggest, matching demand and maintenance data through integrated databases can increase the predictability of service quantities and thereby enhance supply chain effectiveness. Beyond that, studies have begun to analyze interactive data sources such as social media networks (Chae, 2015) as well as more interactive methods of information visualization such as social network analysis (Basole and Bellamy, 2014) only sporadically.

Research framework and future research directions

Based on our systematic literature review, we identified several major research gaps regarding the role of IT in SCRM. First, while much research has investigated operational supply chain risk, fewer insights are available regarding the concrete sources of disruption risk beyond managing information supply chains in the aftermath of disasters. Second, most research focuses on employing IT for risk reduction, whereas insights on other aspects of risk management are sparse and rather fragmented. And third, most of the reviewed articles focus on the potential of IT for sharing and providing information; only a few researchers have investigated the impact of risk on other constituents of a supply chain, such as physical products and materials. In particular, we lack insights into the specific effects of disruption risk on these supply chain constituents.

To provide further guidance on these issues and provide insights from a practitioner perspective, we discussed the review findings and current practices, benefits and issues of integrating SCRM and IT with senior employees and supply chain experts from German companies that participated in an international research project. Based on our discussions, we developed a framework that compares supply chain risk sources, their implications for physical supply chain flows and potential IT strategies with which they might be addressed. In contrast to most existing research on the topic, practitioners stressed the importance of disruptions as potential causes of supply chain risk. Extending the conceptual background of our work, this insight makes it necessary to differentiate between *natural and environmental* causes of disruptions, such as floods, earthquakes and environmental pollution, and *human-made* hazards that cause disruptions, which may be caused by negligence or errors but are *unintentional*, and those that are *intentional*, as in the case of terrorist attacks or product sabotage (Stoneburner *et al.*, 2002). This distinction between natural and human-made risk sources is also reflected in articles that discuss disruption risk in terms of both the hazards that cause them (Gatignon *et al.*, 2010) – as opposed to studies investigating risks that arise from supply chain entities' handling of these disruptions, such as delays in reporting (Gopalakrishna-Remani *et al.*, 2018) – and factors that generally increase supply chains' vulnerability to these hazards (Pettit *et al.*, 2010). This classification is also suggested by evidence from the crisis management literature (Eshghi and Larson, 2008).

Practitioners emphasized as well the need to distinguish more specifically between the potential impacts of risk on physical supply chain flows (e.g. raw materials, semifinished or finished products). Two categories of risk impacts emerged from our discussions: one that concerns physical goods not present along the supply chain because, for instance, they have not been produced or are not needed; and another that concerns goods that are present. The latter is divided further in two subcategories. First, even if relevant goods are present, disruptions can prevent their delivery, for example, due to transportation issues such as impassable roads or traffic jams. This subcategory also includes technical issues that prevent the transportation or sale of goods, such as the breakdown of critical infrastructures. Second, goods that are present can be harmful if they are somehow affected by disruptions and therefore not acceptable for sale, available for delivery or lack warranty. Issues of this sort are salient particularly in industries in which goods and services can present an immediate danger to consumers, such as in the healthcare, agri-food and manufacturing domains.

Combining these categories' results in a framework with nine research areas, each a specific constellation of risk source and impact in supply chains requiring different strategies to deal with the related problems. IT can serve various purposes in helping to identify, analyze, reduce and monitor risk in each constellation. There are also specific requirements for IT to support these strategies. In Table 5, we propose research directions for each of the framework's research areas. The cells in gray include issues that have already been researched but for which some research gaps remain. Cells in white are areas that require the most attention for future research.

		Risk source		
		Human-made		Natural/Environmental
Risk impact		Intentional	Unintentional	
Goods available	Harmful goods	Improvement of supporting IT for quickly tracking deviations and enabling comparisons with competitors and partnersProtection of possible points of attack through adequate security initiatives	Application of new IT for risk monitoring and detectionIdentification of affected goods and quick execution of product recalls	Real-time availability of consistent and reliable information to contain crisesSupply-chain-wide integration of joint activitiesImprovement of supply chain operations and responses to public health disruptions
	Delivery not possible	Improvement and application of commonly used information systems in the industryUse of IT for geographical positioning, transport unit identification and information sharing	Improvement of coordination and cooperation for better responsiveness through interorganizational ITUse of open standards to reduce relationship specificity and enable connections to more partners	Real-time identification of scope and magnitude of impactsApproaches for quickly building or rebuilding supply chains
Goods not available		Application of policies, procedures and IT to protect supply chain assets from theft, damage and terrorismConsideration of alternative supply chain approaches to avoid various sources of disruption	Improvement and utilization of tools and techniques for risk identification and minimizationIncentive mechanisms and coordination approaches for investing in IT	Integration of databases for recovering information, allocating resources and avoiding supply chain shortfallsApproaches for quickly restructuring supply chains and prioritizing commodity flows

Table 5.
Research framework and research directions

The table shows that harmful, modified or damaged products are a major issue in SCRM practice. Little if any research exists regarding potential applications of IT to deal with intentional human-made and different types of natural risk sources that impair physical goods (as opposed to interfering with the interorganizational integration of information flows). To prevent intentional human activities that lead to such products, IT could help with security initiatives aimed at protecting possible points of attack along the supply chain. Options range from simple solutions, such as conditional access rights, to the systematic monitoring of critical areas. Directly associated is the development of supporting information systems, such as alert and reporting systems. Those systems should be able to detect deviations and enable firms to compare their products with competitors or supply chain partners anonymously to identify problems and specify their origins quickly within the supply chain. While identifying and monitoring potentially harmful modifications could be based on existing technologies, such as RFID and integration of information systems and databases, organizational IT applications will probably be less useful for tracking human error or wrongdoing beyond the workplace. Monitoring social media to identify cases of intentional or unintentional food contamination (Newkirk *et al.*, 2012) is an example of an IT strategy that could fill this gap but is not yet prominently discussed in SCM research.

Unintentional disruptions and incidents from natural risk sources that lead to harmful or defective products cannot be precluded. In critical industries such as pharmaceuticals, firms already utilize advanced technologies to monitor quality requirements and detect problems. Research could focus on how to adapt and improve these technologies for other industries. Further, product recalls are a frequent issue in SCM. Rapid identification of affected products and quick implementation of product recalls are often mentioned as problems because of insufficient tracking and tracing along the entire supply chain – extremely important for efficient supply chain operations, especially through real-time availability of consistent and reliable information during a product-recall crisis. The most important prerequisite for achieving efficient tracking and tracing is supply-chain-wide integration of joint activities between supply chain partners. Further research on interorganizational IT is needed to improve information and physical flows in the entire supply chain. In addition, for disruptions that affect public health, supply chain operations not only need to meet business demands but must also focus on responding to public needs. While prior research has by and large focused on existing solutions such as RFID for monitoring goods and products, IT that provides timely information about potential risks and decision support could help to reduce risks also once they have been identified.

When delivery of goods is not possible due to transportation or other problems, the entire supply chain is easily paralyzed, even if only temporarily. Future research could focus on IT solutions to identify the scope and magnitude of different types of disruptions. Evidence from other fields of research suggests that business intelligence applications, for instance, could serve as early warning systems to identify risks and help analyze and make sense of risk, such as by monitoring financial transactions, applying text mining techniques to audit transcripts or using simulation models to monitor the evolution of complex risks (Wu *et al.*, 2014). In the field of crisis informatics, volunteered location information (e.g. from social media or crowdsourcing platforms) is becoming increasingly relevant for identifying emerging security threats and public responses to events (Haworth and Bruce, 2015). Furthermore, promising insights for researchers and practitioners could also lie in research on solutions and approaches for quickly building or rebuilding not only information but also product supply chains, in response to crisis situations – with the objective of continuing operations. In the domain of operations research, we find research over a long period on the tasks required in the aftermath of a disaster or crisis event (Altay and Green, 2006), yet studies we reviewed that investigate the role of IT in such situations have focused mostly on setting up efficient information supply chains (e.g. Day *et al.*, 2009).

For situations in which goods are not available, research could explore approaches to integrating databases to recover information, allocate resources and avoid further supply chains shortfalls. Furthermore, risk impacts force firms to compensate quickly for supply shortfalls, such as by distributing alternative goods. Again, insights into the management of humanitarian and disaster relief supply chains might be transferable to an industrial context to inform the setup of information supply chains after disruptions. But research still lacks methods for quickly restructuring physical supply chains and prioritizing urgently needed goods. Finally, if goods are not available due to intentional human activities, research could close a gap by exploring policies, procedures and technologies to protect supply chain assets from theft, damage and terrorism. Such support could include, for example, comprehensively monitoring critical areas or operations with the help of intelligent devices. Research could also consider supply chain design options aimed at avoiding various disruption sources that result from intentional human action.

There is already notable research activity in the areas shown in Table 5's gray cells. This is particularly true with respect to supply chain shortfalls that arise in the aftermath of natural disaster events, when supply chains have to first be established and required goods are not (yet) available on site (e.g. Charles *et al.*, 2016). IT requirements investigated in this research area can, for instance, support monitoring and integration of information supply chains (Day *et al.*, 2009). In addition, effective IT-enabled decentralized information supply chains have been found to monitor rare infectious diseases and thus reduce the risk of them spreading (Gopalakrishna-Remani *et al.*, 2018). Finally, supply chains in the agri-food industry, where the risk of unintentionally spoiled goods is commonplace (e.g. Scholten and Schilder, 2015), have been the topic of prior research and fall into the category of unintentional human-made risk sources. Nevertheless, there remain research gaps to close and future directions to explore. As the results from our literature review suggest, most articles investigate operational risk sources, such as delivery and transportation issues. These problems are often associated with interorganizational information systems. Future research could focus on improving the coordination and cooperation mechanisms underlying these systems' responsiveness. Although the use of IT for locational positioning, transport unit identification and information sharing is already at an advanced stage, there are still challenges for comprehensive supply-chain-wide solutions.

Moreover, unintentional incidents often lead to disruptions in supply chains that can result in supply shortfalls. Quality management activities are aimed at preventing such problems, a topic some articles address. Following their suggestions, incentive mechanisms and coordination approaches for investing in IT should be investigated further (Fawcett *et al.*, 2007; Klein and Rai, 2009). Advanced planning systems and supply chain event management are good examples of tools for identifying and minimizing disruption risk in supply chains.

Conclusion

In this article, we provide an overview of representative articles investigating IT for SCRM, including a classification of current approaches and a critical discussion of research trends and gaps. Building upon the findings of our literature review and insights from practitioners involved in a three-year international research project, we propose a research framework for addressing the gaps.

Our literature review's main contribution is the identification of three primary research gaps regarding IT in SCRM. First, most research investigates the potential of IT for supply chain risk reduction, while few articles address IT support for risk identification, analysis and monitoring. Second, there is a lack of research on specific sources of disruption risk and how IT can help in managing those risks, especially with respect to the management of business-related supply chains. And third, the focus of research has been on the potential of IT to enable information provision and sharing, thus neglecting risk for products and materials in a supply chain. To address these issues, we propose a framework that focuses on the effect of disruption risk on physical supply chain flows. We identify nine supply chain risk constellations based on risk sources and impacts and suggest promising research approaches for each constellation.

The major limitation of our work concerns the literature search process, as we restricted our search to highly relevant outlets. Thus, while the sample of articles analyzed is representative of research on SCRM, it is not comprehensive. Furthermore, while we utilized a rather inclusive list of keywords, we cannot preclude that we missed relevant articles. Future reviews could aim at a comprehensive rather than representative sample of articles.

Supply chain disruptions are a major source of risk for business organizations and consumers alike. From both practical and research perspectives, current knowledge of how to avoid and manage supply chain risk and disruptions with the support of IT is insufficient. Our review provides a useful starting point for future research in this area by integrating perspectives and research opportunities on IT support for handling disruption risk for both information and physical supply chain flows.

References

Aiello, G., Enea, M. and Muriana, C. (2015), "The expected value of the traceability information", *European Journal of Operational Research*, Vol. 244 No. 1, pp. 176-186.

Altay, N. and Green, W.G. (2006), "OR/MS research in disaster operations management", *European Journal of Operational Research*, Vol. 175 No. 1, pp. 475-493.

Australian Business Deans Council (2016), "ABDC journal quality list," available at: http://www.abdc.edu.au/master-journal-list.php (accessed 28 April 2017).

Bandara, W., Furtmueller, E., Gorbacheva, E., Miskon, S. and Beekhuyzen, J. (2015), "Achieving rigor in literature reviews. Insights from qualitative data analysis and tool-support", *Communications of the Association for Information Systems*, Vol. 34, article 8, pp. 154-204.

Bandyopadhyay, K., Mykytyn, P.P. and Mykytyn, K. (1999), "A framework for integrated risk management in information technology", *Management Decision*, Vol. 37 No. 5, pp. 437-445.

Basole, R.C. and Bellamy, M.A. (2014), "Visual analysis of supply network risks. Insights from the electronics industry", *Decision Support Systems*, Vol. 67, pp. 109-120.

Blackman, I.D., Holland, C.P. and Westcott, T. (2013), "Motorola's global financial supply chain strategy", *Supply Chain Management: An International Journal*, Vol. 18 No. 2, pp. 132-147.

Brandon-Jones, E., Squire, B., Autry, C.W. and Petersen, K.J. (2014), "A contingent resource-based perspective of supply chain resilience and robustness", *Journal of Supply Chain Management*, Vol. 50 No. 3, pp. 55-73.

Cannon, A.R., Reyes, P.M., Frazier, G.V. and Prater, E.L. (2008), "RFID in the contemporary supply chain: multiple perspectives on its benefits and risks", *International Journal of Operations & Production Management*, Vol. 28 No. 5, pp. 433-454.

Chae, B. (2015), "Insights from hashtag #supplychain and Twitter analytics. Considering Twitter and Twitter data for supply chain practice and research", *International Journal of Production Economics*, Vol. 165, pp. 247-259.

Charles, A., Lauras, M., van Wassenhove, L.N. and Dupont, L. (2016), "Designing an efficient humanitarian supply network", *Journal of Operations Management*, Vol. 47-48, pp. 58-70.

Chen, R., Sharman, R., Chakravarti, N., Rao, H.R. and Upadhyaya, S.J. (2008), "Emergency response information system interoperability. Development of chemical incident response data model", *Journal of the Association for Information Systems*, Vol. 9 No. 3/4, pp. 200-230.

Chopra, S. and Sodhi, M.S. (2004), "Managing risk to avoid supply-chain breakdown", *MIT Sloan Management Review*, Vol. 46 No. 1, p. 53.

Chow, H.K.H., Choy, K.L., Lee, W.B. and Chan, F.T.S. (2007), "Integration of web-based and RFID technology in visualizing logistics operations. A case study", *Supply Chain Management: An International Journal*, Vol. 12 No. 3, pp. 221-234.

Colicchia, C., Creazza, A. and Menachof, D.A. (2018a), "Managing cyber and information risks in supply chains: insights from an exploratory analysis", *Supply Chain Management: An International Journal*, Vol. 17 No. 2, p. 93.

Colicchia, C., Creazza, A., Noè, C. and Strozzi, F. (2018b), "Information sharing in supply chains: a review of risks and opportunities using the systematic literature network analysis (SLNA)", *Supply Chain Management: An International Journal*, Vol. 50 No. 3, p. 55.

Coronado Mondragon, A.E., Lalwani, C.S., Coronado Mondragon, E.S. and Coronado Mondragon, C.E. (2009), "Facilitating multimodal logistics and enabling information systems connectivity through wireless vehicular networks", *International Journal of Production Economics*, Vol. 122 No. 1, pp. 229-240.

Day, J.M., Junglas, I. and Silva, L. (2009), "Information flow impediments in disaster relief supply chains", *Journal of the Association for Information Systems*, Vol. 10 No. 8, pp. 637-660.

Deshpande, V., Iyer, A.V. and Cho, R. (2006), "Efficient supply chain management at the US coast guard using part-age dependent supply replenishment policies", *Operations Research*, Vol. 54 No. 6, pp. 1028-1040.

d'Aubeterre, F., Singh, R. and Iyer, L. (2008), "A semantic approach to secure collaborative inter-organizational eBusiness processes (SSCIOBP)", *Journal of the Association for Information Systems*, Vol. 9 Nos 3/4, p. 231.

Erasmus Research Institute of Management. (2016), "*ERIM Journals List (EJL) 2016-2021*", available at: https://www.erim.eur.nl/about-erim/erim-journals-list-ejl/ (accessed 28 April 2017).

Eshghi, K. and Larson, R.C. (2008), "Disasters: lessons from the past 105 years", *Disaster Prevention and Management: An International Journal*, Vol. 17 No. 1, pp. 62-82.

Fan, H., Li, G., Sun, H. and Cheng, T.C.E. (2017), "An information processing perspective on supply chain risk management: antecedents, mechanism, and consequences", *International Journal of Production Economics*, Vol. 185, pp. 63-75.

Fawcett, S.E., Osterhaus, P., Magnan, G.M., Brau, J.C. and McCarter, M.W. (2007), "Information sharing and supply chain performance. The role of connectivity and willingness", *Supply Chain Management: An International Journal*, Vol. 12 No. 5, pp. 358-368.

Ford, E.W. and Hughes, J.A. (2007), "A collaborative product commerce approach to value-based health plan purchasing", *Supply Chain Management: An International Journal*, Vol. 12 No. 1, pp. 32-41.

Gatignon, A., van Wassenhove, L.N. and Charles, A. (2010), "The Yogyakarta earthquake: humanitarian relief through IFRC's decentralized supply chain", *International Journal of Production Economics*, Vol. 126 No. 1, pp. 102-110.

Ghadge, A., Dani, S. and Kalawsky, R. (2012), "Supply chain risk management: present and future scope", *International Journal of Logistics Management*, Vol. 23 No. 3, pp. 313-339.

Giannakis, M. and Louis, M. (2011), "A multi-agent based framework for supply chain risk management", *Journal of Purchasing and Supply Management*, Vol. 17 No. 1, pp. 23-31.

Gonul Kochan, C., Nowicki, D.R., Sauser, B. and Randall, W.S. (2018), "Impact of cloud-based information sharing on hospital supply chain performance: a system dynamics framework", *International Journal of Production Economics*, Vol. 195, pp. 168-185.

Gopalakrishna-Remani, V., Brown, J.R., Shanker, M. and Hu, M. (2018), "An information supply chain system view for managing rare infectious diseases: the need to improve timeliness", *Information & Management*, Vol. 55 No. 2, pp. 215-223.

Gunasekaran, A., Ngai, E.W.T. and McGaughey, R.E (2006), "Information technology and systems justification. a review for research and applications", *European Journal of Operational Research*, Vol. 173 No. 3, pp. 957-983.

Gupta, S., Starr, M.K., Farahani, R.Z. and Matinrad, N. (2016), "Disaster management from a POM perspective: mapping a new domain, *Production and Operations Management*, Vol. 25 No. 10, pp. 1611-1637.

Hall, D.J., Skipper, J.B., Hazen, B.T. and Hanna, J.B. (2012), "Inter-organizational IT use, cooperative attitude, and inter-organizational collaboration as antecedents to contingency planning effectiveness", *International Journal of Logistics Management*, Vol. 23 No. 1, pp. 50-76.

Haworth, B. and Bruce, E. (2015), "A review of geographic information for disaster management", *Geography Compass*, Vol. 9 No. 5, pp. 237-250.

Ho, W., Zheng, T., Yildiz, H. and Talluri, S. (2015), "Supply chain risk management: a literature review", *International Journal of Production Research*, Vol. 53 No. 16, pp. 5031-5069.

Jede, A. and Teuteberg, F. (2016), "Towards cloud-based supply chain processes. Designing a reference model and elements of a research agenda", *International Journal of Logistics Management*, Vol. 27 No. 2, pp. 438-462.

Jiang, L., Dimitrov, S. and Mantin, B. (2017): "P2P marketplaces and retailing in the presence of consumers' valuation uncertainty", *Production and Operations Management,* Vol. 26 No. 3, pp. 509-524.

Jüttner, U., Peck, H. and Christopher, M. (2003), "Supply chain risk management. Outlining an agenda for future research", *International Journal of Logistics: Research and Applications*, Vol. 6 No. 4, pp. 197-210.

Kembro, J.H., Danielsson, V. and Smajli, G. (2017), "Network video technology: exploring an innovative approach to improving warehouse operations", *International Journal of Physical Distribution & Logistics Management*, Vol. 47 No. 7, pp. 623-645.

Klein, R. and Rai, A. (2009), "Interfirm strategic information flows in logistics supply chain relationships", *MIS Quarterly*, Vol. 33 No. 4, pp. 735-762.

Knemeyer, A.M., Zinn, W. and Eroglu, C. (2009), "Proactive planning for catastrophic events in supply chains", *Journal of Operations Management*, Vol. 27 No. 2, pp. 141-153.

Kunz, N., Reiner, G. and Gold, S. (2014), "Investing in disaster management capabilities versus pre-positioning inventory. A new approach to disaster preparedness", *International Journal of Production Economics*, Vol. 157, pp. 261-272.

Lavastre, O., Gunasekaran, A. and Spalanzani, A. (2012), "Supply chain risk management in French companies", *Decision Support Systems,* Vol. 52 No. 4, pp. 828-838.

Lee, J., Palekar, U.S. and Qualls, W. (2011), "Supply chain efficiency and security. Coordination for collaborative investment in technology", *European Journal of Operational Research*, Vol. 210 No. 3, pp. 568-578.

Leonardi, P.M., Huysman, M. and Steinfield, C. (2013), "Enterprise social media: definition, history, and prospects for the study of social technologies in organizations", *Journal of Computer-Mediated Communication*, Vol. 19 No. 1, pp. 1-19.

Levermore, D.M., Babin, G. and Hsu, C. (2010), "A new design for open and scalable collaboration of independent databases in digitally connected enterprises", *Journal of the Association for Information Systems*, Vol. 11 No. 7, pp. 367-393.

Luftman, J., Derksen, B., Dwivedi, R., Santana, M., Zadeh, H.S. and Rigoni, E. (2015), "Influential IT management trends. an international studies", *Journal of Information Technology*, Vol. 30 No. 3, pp. S293-S305.

Machado, S.M., Paiva, E.L. and da Silva, E.M. (2018), "Counterfeiting: addressing mitigation and resilience in supply chains", *International Journal of Physical Distribution & Logistics Management*, Vol. 48 No. 2, pp. 139-163.

Manuj, I. and Mentzer, J.T. (2008), "Global supply chain risk management strategies", *International Journal of Physical Distribution & Logistics Management*, Vol. 38 No. 3, pp. 192-223.

Maon, F., Lindgreen, A. and Vanhamme, J. (2009), "Developing supply chains in disaster relief operations through cross-sector socially oriented collaborations. A theoretical model", *Supply Chain Management: An International Journal*, Vol. 14 No. 2, pp. 149-164.

Mei, Z. and Dinwoodie, J. (2005), "Electronic shipping documentation in China's international supply chains", *Supply Chain Management: An International Journal*, Vol. 10 No. 3, pp. 198-205.

Meijboom, B., Schmidt-Bakx, S. and Westert, G. (2011), "Supply chain management practices for improving patient-oriented care", *Supply Chain Management: An International Journal*, Vol. 16 No. 3, pp. 166-175.

Newkirk, R.W., Bender, J.B. and Hedberg, C.W. (2012), "The potential capability of social media as component of food safety and food terrorism surveillance systems", *Foodborne Pathogens and Disease*, Vol. 9 No. 2, pp. 120-124.

Norrman, A. and Jansson, U. (2004), "Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident", *International Journal of Physical Distribution & Logistics Management*, Vol. 34 No. 5, pp. 434-456.

Olorunniwo, F.O. and Li, X. (2010), "Information sharing and collaboration practices in reverse logistics", *Supply Chain Management: An International Journal*, Vol. 15 No. 6, pp. 454-462.

Paré, G., Trudel, M.-C., Jaana, M. and Kitsiou, S. (2015), "Synthesizing information systems knowledge. A typology of literature reviews", *Information & Management*, Vol. 52 No. 2, pp. 189-199.

Paré, G., Tate, M., Johnstone, D. and Kitsiou, S. (2016), "Contextualizing the twin concepts of systematicity and transparency in information systems literature reviews", *European Journal of Information Systems*, Vol. 25 No. 6, pp. 493-508.

Pettit, T.J., Fiksel, J. and Croxton, K.L. (2010), "Ensuring supply chain resilience: development of a conceptual framework", *Journal of Business Logistics*, Vol. 31 No. 1, pp. 1-21.

Pibernik, R., Zhang, Y., Kerschbaum, F. and Schröpfer, A. (2011), "Secure collaborative supply chain planning and inverse optimization – the JELS model", *European Journal of Operational Research*, Vol. 208 No. 1, pp. 75-85.

Power, D. (2005), "Supply chain management integration and implementation: a literature review", *Supply Chain Management: An International Journal*, Vol. 10 No. 4, pp. 252-263.

Puschmann, T. and Alt, R. (2005), "Successful use of e-procurement in supply chains", *Supply Chain Management: An International Journal*, Vol. 10 No. 2, pp. 122-133.

Raisinghani, M.S. and Meade, L.L. (2005), "Strategic decisions in supply-chain intelligence using knowledge management: an analytic-network-process framework", *Supply Chain Management: An International Journal*, Vol. 10 No. 2, pp. 114-121.

Richey, R.G. and Autry, C.W. (2009), "Assessing interfirm collaboration/technology investment tradeoffs", *International Journal of Logistics Management,* Vol. 20 No. 1, pp. 30-56.

Riley, J.M., Klein, R., Miller, J. and Sridharan, V. (2016), "How internal integration, information sharing, and training affect supply chain risk management capabilities", *International Journal of Physical Distribution & Logistics Management*, Vol. 46 No. 10, pp. 953-980.

Ringsberg, H. (2014), "Perspectives on food traceability: a systematic literature review", *Supply Chain Management: An International Journal*, Vol. 19 No. 5/6, pp. 558-576.

Sambhara, C., Rai, A. and Xu, S.X. (2016), "Enterprise system implementations: role of information risk, internal controls and environmental uncertainty", in *Proceedings of the International Conference on Information Systems*, Dublin.

Scholten, K. and Schilder, S. (2015), "The role of collaboration in supply chain resilience", *Supply Chain Management: An International Journal*, Vol. 20 No. 4, pp. 471-484.

Sheffi, Y. (2001), "Supply chain management under the threat of international terrorism", *International Journal of Logistics Management*, Vol. 12 No. 2, pp. 1-11.

Shi, D. (2004), "A review of enterprise supply chain risk management", *Journal of Systems Science and Systems Engineering*, Vol. 13 No. 2, pp. 219-244.

Simangunsong, E., Hendry, L.C. and Stevenson, M. (2012), "Supply-chain uncertainty: a review and theoretical foundation for future research", *International Journal of Production Research*, Vol. 50 No. 16, pp. 4493-4523.

Skipper, J.B. and Hanna, J.B. (2009), "Minimizing supply chain disruption risk through enhanced flexibility", *International Journal of Physical Distribution & Logistics Management*, Vol. 39 No. 5, pp. 404-427.

Stoneburner, G., Goguen, A.Y. and Feringa, A. (2002), *Risk Management Guide for Information Technology Systems*, Technical Report SP 800-30, National Institute of Standards and Technology, Gaithersburg, MD.

Tang, C.S. (2006), "Perspectives in supply chain risk management", *International Journal of Production Economics*, Vol. 103 No. 2, pp. 451-488.

Taylor, D.H. and Fearne, A. (2006), "Towards a framework for improvement in the management of demand in agri-food supply chains", *Supply Chain Management: An International Journal*, Vol. 11 No. 5, pp. 379-384.

Trkman, P. and McCormack, K. (2009), "Supply chain risk in turbulent environments—a conceptual model for managing supply chain network risk", *International Journal of Production Economics*, Vol. 119 No. 2, pp. 247-258.

Tummala, V.M.R. and Schoenherr, T. (2008), "Best practices for the implementation of supply chain management initiatives", *International Journal of Logistics Systems and Management*, Vol. 4 No. 4, pp. 391-410.

Urciuoli, L. and Hintsa, J. (2016), "Adapting supply chain management strategies to security - an analysis of existing gaps and recommendations for improvement", *International Journal of Logistics: Research and Applications*, Vol. 20 No. 3, pp. 276-295.

Vanany, I., Zailani, S. and Pujawan, N. (2010), "Supply chain risk management: literature review and future research", *International Journal of Information Systems and Supply Chains*, Vol. 2 No. 1.

Varma, T.N. and Khan, D.A. (2014), "Information technology in supply chain management", *Journal of Supply Chain Management Systems*, Vol. 3 No. 3, pp. 35-46.

Varma, T.N. and Khan, D.A. (2017), "SAP system as vendor fraud detector", *Journal of Supply Chain Management Systems*, Vol. 6 No. 2, pp. 1-13.

Verband der Hochschullehrer für Betriebswirtschaft (2015), "VHB-Jourqual 3", available at: http://vhbonline.org/vhb4you/jourqual/vhb-jourqual-3/ (accessed 28 April 2017).

Wagner, S.M. and Bode, C. (2008), "An empirical examination of supply chain performance along several dimensions of risk", *Journal of Business Logistics*, Vol. 29 No. 1, pp. 307-325.

Wagner, S.M. and Neshat, N. (2010), "Assessing the vulnerability of supply chains using graph theory", *International Journal of Production Economics*, Vol. 126 No. 1, pp. 121-129.

Webster, J. and Watson, R.T. (2002), "Analyzing the past to prepare for the future. Writing a literature review", *MIS Quarterly*, Vol. 26 No. 2, pp. 13-23.

Wu, D.D., Chen, S.-H. and Olson, D.L. (2014), "Business intelligence in risk management. Some recent progresses", *Information Sciences*, Vol. 256, pp. 1-7.

Xie, Y., Breen, L., Cherrett, T., Zheng, D. and Allen, C.J. (2016), "An exploratory study of reverse exchange systems used for medical devices in the UK national health service", *Supply Chain Management: An International Journal,* Vol. 21 No. 2, pp. 194-215.

Yang, Z., Aydın, G., Babich, V. and Beil, D.R. (2009), "Supply disruptions, asymmetric information, and a backup production option", *Management Science*, Vol. 55 No. 2, pp. 192-209.

Yang, L., Su, G. and Yuan, H. (2012), "Design principles of integrated information platform for emergency responses: the case of 2008 Beijing Olympic Games", *Information Systems Research*, Vol. 23 No. 3-part-1, pp. 761-786.

Corresponding author
Diana Fischer-Preßler can be contacted at: Diana.Fischer-Pressler@uni-bamberg.de