Institutional Environments and Conflict Between Foreign Investors and Local Communities in Large-scale Agricultural Land Acquisitions

Ueta, Toshimitsu

Document Version
Final published version

Published in:
International Business Review

DOI:
10.1016/j.ibusrev.2024.102319

Publication date:
2024

Building supply chain resilience to cyber risks: a dynamic capabilities perspective

Michael Herburger
Department of Logistikum, University of Applied Sciences Upper Austria – Campus Steyr, Steyr, Austria
Andreas Wieland
Department of Operations Management, Copenhagen Business School, Frederiksberg, Denmark, and
Carina Hochstrasser
Department of Logistikum, University of Applied Sciences Upper Austria – Campus Steyr, Steyr, Austria

Abstract

Purpose – Disruptive events caused by cyber incidents, such as supply chain (SC) cyber incidents, can affect firms' SC operations on a large scale, causing disruptions in material, information and financial flows and impacting the availability, integrity and confidentiality of SC assets. While SC resilience (SCRES) research has received much attention in recent years, the purpose of this study is to investigate specific capabilities for building SCRES to cyber risks. Based on a nuanced understanding of SC cyber risk characteristics, this study explores how to build SC cyber resilience (SCCR) using the perspective of dynamic capability (DC) theory.

Design/methodology/approach – Based on 79 in-depth interviews, this qualitative study examines 28 firms representing 4 SCs in Central Europe. The researchers interpret data from semistructured interviews and secondary data using the DC perspective, which covers sensing, seizing and transforming.

Findings – The authors identify SCRES capabilities, in general, and SCCR-specific capabilities that form the basis for the realignment of DCs for addressing cyber risks in SCs. The authors argue that SCRES capabilities should, in general, be combined with specific capabilities for SCCR to deal with SC cyber risks. Based on these findings, 10 propositions for future research are provided.

Practical implications – Practitioners should collaborate specifically to address cyber threats and risks in SCs, integrate new SC partners and use new approaches. Furthermore, this study shows that cyber risks need to be treated differently from traditional SC risks.

Originality/value – This empirical study enriches the SC management literature by examining SCRES to cyber risks through the insightful lens of DCs. It identifies DCs for building SCCR, makes several managerial contributions and is among the few that apply the DC approach to address specific SC risks.

Keywords Supply chain resilience, Cyber risks, Dynamic capabilities

Paper type Case study

Introduction

As supply chains (SCs) are likely at more risk than ever before because of today's complex business environment, research on SC resilience (SCRES) to understand the changes caused by threats and risks has become crucial (Wieland *et al.*, 2023). The current business environment, with its increasing reliance on networked digital systems, increases the importance of understanding cyber risks within SCs (Zouari *et al.*, 2021). As a result, many capabilities have been identified and acknowledged as necessary for building and improving SCRES in general (Christopher and Peck, 2004; Pettit *et al.*, 2010; Scholten *et al.*, 2014; Pettit *et al.*, 2019; Han *et al.*, 2020; Nikookar *et al.*, 2024). Although the SCRES literature has grown tremendously over the past decade and emphasizes disruptions caused by natural disasters (Oke and Nair, 2023), research focusing on capabilities that are relevant to specific SC risks is scarce (Tukamuhabwa *et al.*, 2015), such as for managing SC cyber threats (Colicchia *et al.*, 2019; Ghadge *et al.*, 2019, Melnyk *et al.*, 2022).

While Walker (2020) highlights the importance of considering the system's general and specific resilience, addressing cyber risks in the SCRES literature is underrepresented (Melnyk *et al.*, 2022). However, cyber risks were among the top risks for companies and SCs in 2023, as cyber attacks have been affecting a rising number of organizations of all sizes, sectors and locations (ENISA, 2022; Allianz, 2023). Given the increasing cyber threats

The current issue and full text archive of this journal is available on Emerald Insight at: **https://www.emerald.com/insight/1359-8546.htm**

Supply Chain Management: An International Journal
29/7 (2024) 28–50
Emerald Publishing Limited [ISSN 1359-8546]
[DOI 10.1108/SCM-01-2023-0016]

This project is co-financed by research subsidies granted by the government of Upper Austria.

Received 13 January 2023
Revised 18 July 2023
23 October 2023
1 February 2024
16 April 2024
Accepted 17 April 2024

Supply Chain Management: An International Journal
Volume 29 · Number 7 · 2024 · 28–50

and the profound impact they can have on SCs, there is an evident need to delve deeper into this area.

Nevertheless, due to the lack of addressing and understanding cyber risks in SCs, it remains unclear which DCs support SCs in building and improving SCRES for cyber threats. This specific consideration of SCRES capabilities for cyber risks is essential due to the different characteristics and divergent impacts from those usually discussed in SCs (Melnyk *et al.*, 2022). For example, while traditionally investigated risks (e.g. natural disasters) mainly harm the availability of SC assets, cyber risks have the potential to simultaneously impact the availability, integrity and confidentiality of SC assets because systems and the data within them can be altered and spied upon for months without notice. Information retrieved from these attacks can then be used to attack SC partners, combining two attacks into one SC cyber attack, causing damage to whole sectors and SCs, as seen in previous cases, such as those on SolarWinds and Kaseya (ENISA, 2022).

The cumulative impact of these threats can disrupt not only individual SCs but also entire industries or regions, which emphasizes the urgency of developing a theoretical framework based on SCRES that has focus specifically on cyber risk, which is the aim of this study. The lack of awareness and understanding of cyber risks and the SCRES literature's focus on the material flow of goods probably explains why firms have difficulties addressing cyber risks in SCs (Melnyk *et al.*, 2022). In addition, successfully mitigating cyber risks in the SC requires an interdisciplinary approach that combines different DCs, appropriate skills, technological expertise and human factors (Bartol, 2014; Strupczewski, 2021) – an approach that has not yet been established in firms. Therefore, it is crucial to identify and understand the capabilities needed to facilitate SCRES to cyber risks from both SC management (SCM) and information technology (IT). Furthermore, a combination of relevant specific and general SCRES capabilities is necessary for fully addressing cyber risks in SCs. Given this background, the research question becomes even more urgent and relevant. These arguments lead to the following research question:

RQ1. How can SCs sense and respond to cyber risks to facilitate SCRES?

Acknowledging that cyber risk-related strategies are usually outside most SC executives' core activities, the challenge is creating new managerial and organizational capabilities for building SCRES to address cyber risks. Dynamic capability (DC) theory often refers to the recreation of managerial and organizational capabilities (Teece *et al.*, 1997; Teece, 2007) and is one of the most taken lenses to study SCRES phenomena (Tukamuhabwa *et al.*, 2015; Kochan and Nowicki, 2018; Ali and Gölgeci, 2019; Bahrami and Shokouhyar, 2022). This theory focuses on how firms undertake activities and adjust their resources and competencies in response to environmental changes. This study develops DC theory for analyzing SCRES to address cyber risks, which complements SCRES studies. Data are interpreted from semistructured interviews and secondary data, which covers sensing, seizing and transforming and allows a hierarchical view of the identified capabilities.

A multicase study research design involving key SCM and IT security actors from 28 firms in four industrial SCs in Central Europe, representing three SC triads and one with tetradic relation (Durach *et al.*, 2020), is used to answer the study's research question by combining interdisciplinary expertise from a managerial point of view. These specific firms and SCs were chosen as they identify digitalization as a business core activity that lacks focus on cyber threats and risks. By analyzing the cyber resilience of SCs, we elaborate on DC theory introduced by Teece *et al.* (1997) and refined by Teece (2007) and examine existing explanations in SCRES in the context of Central Europe. Consequently, this study demonstrates that DC provides a sound theoretical lens for advancing the knowledge of management practices to build SCRES for cyber risks.

As a theoretical lens, DC enabled us to investigate the capabilities for facilitating SC cyber resilience (SCCR). The study's perspective informs managers that, for sensing and responding to cyber risks to facilitate SCCR, they should develop and modify specific DCs to address cyber risks in SCs and combine them with DCs developed for SCRES in general.

The remainder of this article is organized as follows. Section 2 presents the theoretical background of the study, including an overview of the relevant literature on SCRES, cyber risks and DC. Section 3 outlines the empirical multicase study research method adopted before the findings are presented in Section 4 and discussed in Section 5. The final section outlines the contribution to theory and practice and provides areas for future research.

Literature review

Supply chain resilience

SCRES is acknowledged as the key ability of SCs to cope with disruptions or changes (Jüttner and Maklan, 2011; Scholten and Schilder, 2015; Wieland and Durach, 2021). Recent examples of such events include the COVID-19 pandemic and the blockage of the Suez-Canal (Ivanov and Das, 2020; Ivanov and Dolgui, 2021; Roh *et al.*, 2022; Wieland *et al.*, 2023). Although resilience was introduced to the context of SCs almost 20 years ago (Rice and Caniato, 2003; Christopher and Peck, 2004), the interpretation of resilience in the SC context is still an ongoing and long-running debate. Various literature reviews have recently examined the variety of SCRES definitions (Tukamuhabwa *et al.*, 2015; Ali *et al.*, 2017; Kochan and Nowicki, 2018; Han *et al.*, 2020).

The literature emphasizes three main types of resilience: engineering, ecological and social-ecological resilience (Holling, 1996; Wieland and Durach, 2021). However, the discussion of these different interpretations of resilience in the SC context has started only recently (Wieland, 2021; Wieland and Durach, 2021). Most scholars have interpreted SCRES as engineering resilience (Richey *et al.*, 2022; Wieland and Durach, 2021), arguing that SCRES relates to the ability of an SC to return to equilibrium after disruption (Holling, 1973; Christopher and Peck, 2004). In contrast, social-ecological resilience is measured by the magnitude of disturbance a system can sustain before an SC changes its control or structure (Holling, 1996; Wieland and Durach, 2021). Furthermore, the SCRES literature primarily focuses on resilience in general, emphasizing mainly natural disasters and the flow of goods. However, it has rarely focused on

specific risks or built strategies for addressing risks individually (Tukamuhabwa *et al.*, 2015), such as cyber risks.

Cyber risks in supply chains

Several scholars emphasize the lack of research on managing cyber risks from an SC perspective (Colicchia *et al.*, 2019; Ghadge *et al.*, 2019; Creazza *et al.*, 2022; Melnyk *et al.*, 2022). Despite increasing research addressing cyber risks to SCs, scholars who define the term are relatively scarce. Although it is acknowledged that information risks and cyber risks are not the same, scholars tend to use these terms interchangeably (von Solms and van Niekerk, 2013). A uniform and broadly accepted definition of cyber risks has not yet emerged (Strupczewski, 2021). In a broad sense, cyber risks are associated with malicious events in cyberspace that result in the loss of a business's reputation and financial resources.

Strupczewski (2021), who studied definitions of cyber risks, concluded that these risks are operational risks to the organization's information, technological assets and resources, with negative consequences to the confidentiality, availability and integrity of these assets. This definition emphasizes the distinction from other risks typically addressed in the SCRES literature, mainly related to material flows, which predominately affect availability. In comparison, cyber risks can additionally and simultaneously harm the confidentiality and integrity of SC assets, information, services and products. Therefore, in this study, SC cyber risks are defined as operational risks associated with executing activities in cyberspace. They adversely impact the integrity, availability and confidentiality of SC assets, information and communication technology resources and technological assets and can damage tangible and intangible SC assets.

Unlike conventional risks, cyber risks have the potential to remain undetectable until their impact on businesses materializes (Renaud *et al.*, 2018). This is why cyber risks are challenging for nonexperts to understand and address (Bravo-Lillo *et al.*, 2011; Jones *et al.*, 2021). Furthermore, the cyber environment allows an attacker to move laterally in entered SC networks, leading to different cascading effects compared to conventional SC risks. By combining two or more cyber attacks, the attackers can potentially harm multiple firms in an SC simultaneously, as numerous SC cyber attacks have demonstrated (ENISA, 2022). Furthermore, it has been argued that the emergence of artificial intelligence, in particular, could lead to an increased risk of cyber attacks (Hendriksen, 2023) that require some form of control to ensure reliable approaches (Taddeo *et al.*, 2019). Daily business in SCs (e.g. highly connected networks with digital infrastructure) depends on SC assets that are at risk of cyber attacks. Building on this understanding of cyber risks in SCs, this research explores how to build SCRES to cyber risks.

Dynamic capabilities

Teece *et al.* (1997) introduced the theory of DCs, which is rooted in the resource-based view of a firm (Wernerfelt, 1984; Barney, 1991). This theory describes a firm's ability to sense and adapt to external environmental changes, which is recognized as crucial to competitiveness. However, the positive impact on firm-level performance is often not directly visible (Drnevich and Kriauciunas, 2011). These external environmental changes are frequently caused by force majeure events, whether foreseeable or not, for better or for worse (Winter, 2003). Teece (2007) identified three microfoundations of DC: sensing, seizing and transforming. Sensing includes scanning, creating, learning and interpreting opportunities and threats. Seizing includes the response to sensed opportunities and threats. Transforming entails reconfiguring assets to enhance, combine or protect companies' capabilities.

While Teece's (2007) sensing, seizing and transforming framework discusses opportunities and threats, this study focuses only on threats. Therefore, this study represents an exceptional understanding of the framework, as most studies focus on opportunities and threats or only on opportunities. Threats and opportunities are not considered opposite ends of the same continuum but are theoretically distinct, which is consistent with the findings of Pérez-Nordtvedt *et al.* (2014) and Endres and van Bruggen (2021). Therefore, this study focuses solely on threats and risks, as threat recognition has a greater impact on revenue growth than sensing opportunities, and firms' common knowledge focuses on opportunities rather than threats (Endres and van Bruggen, 2021).

In the SCM literature, DCs are a competitive necessity in modern business because they help firms respond to environmental challenges and compete in today's business landscape (Ponomarov, 2012). Specifically, in the SCRES literature, DC theory has repeatedly been taken as a lens to investigate SCRES (Tukamuhabwa *et al.*, 2015; Kochan and Nowicki, 2018; Ali and Gölgeci, 2019; Bahrami and Shokouhyar, 2022). Also, data will be interpreted from a DC perspective using three categories: DC allows to show how participants sense the SC to generate an understanding of cyber threats and risks, seize the sensed cyber risks and transform their SC to become more resilient to cyber risks.

SC capabilities are defined as "attributes that enable an enterprise to anticipate and overcome disruptions" (Pettit *et al.*, 2010, p. 6). SC capabilities are related to vulnerabilities listed as interventions in frameworks (Kochan and Nowicki, 2018) and may take several forms, including preventing and mitigating impact and/or enabling firms to adapt after disruptions. The SCRES framework developed by Pettit *et al.* (2010) focuses on balancing SC vulnerabilities and capabilities. It is desirable to establish SCRES by balancing vulnerabilities and capabilities through resilience linkages (Pettit *et al.*, 2013).

Supply chain resilience sensing activities

Sensing, derived from DC theory, involves actively scanning and monitoring the business environment to identify new threats and opportunities. This entails constructing systems to learn, filter and interpret information that supports identifying threats, both at the core and periphery of the business, including those within the SC (Teece, 2007). In the context of SCM, sensing capabilities refer to the proficiency developed from information-sharing practices. These practices keep partners updated about current and anticipated physical flows (Müller and Gaudig, 2011). Integrating such activities can enhance SC practices if the information exchanged relates to operations (Kulp *et al.*, 2004) or risk-related data (Manuj and Mentzer, 2008). Ideally, this exchange of information should be frequent, reciprocal, informal and noncoercive (Vanpoucke *et al.*, 2009). When each SC partner effectively uses the shared information, they can optimize SC dynamics and enhance

decision-making processes. In addition, having access to such information enables a firm to understand what is occurring within the SC and make necessary adaptations (Harland *et al.*, 2007).

Sensing capabilities in SCRES result from situational awareness, visibility and knowledge-creation activities. Situational awareness is the ability to understand SC vulnerabilities and prepare for disruptive events (Datta *et al.*, 2007), which is best achieved through early warning strategies (Sáenz and Revilla, 2014). These practices help map SC vulnerabilities (Melnyk *et al.*, 2010) to prevent or control risks (Manuj and Mentzer, 2008). SC visibility and knowledge management contribute to sensing activities. SC visibility is a crucial aspect of sensing activities, which contributes to SCRES (Scholten and Schilder, 2015; Mubarik *et al.*, 2021) and leads to awareness and knowledge of the current status of SC assets and the surrounding environment (Fiksel *et al.*, 2015) often measured by key performance indicators (Ambulkar *et al.*, 2015). Increased visibility in the SC may be achieved by investing in IT capabilities that facilitate information exchange and communication (Jüttner and Maklan, 2011). In addition, knowledge management and understanding SCs are critical for improving SCRES (Scholten *et al.*, 2014; Umar *et al.*, 2021).

Supply chain resilience seizing activities

While seizing activities support firms in addressing sensed threats and risks (Teece, 2007), SCRES seizing capabilities that are mainly response related (e.g. SC collaboration, agility, flexibility and redundancy) support SCs in addressing sensed threats and risks. Response capabilities enable SCs to react quickly and effectively to SC events, thereby mitigating the impact of disruptions or changes and ensuring a desirable outcome (Ali *et al.*, 2017). SC collaboration increases SCRES (Scholten and Schilder, 2015; Bak *et al.*, 2020) and refers to an SC's ability to respond to disruptions by collaborating with SC partners (Christopher and Peck, 2004) for sharing risk-related information (Jüttner and Maklan, 2011) and coordinating immediate response (Scholten *et al.*, 2014).

SC agility and flexibility contribute to seizing activities. SC agility refers to rapidly reacting to changes, shortages and disruptions. Although SC agility may differ from SCRES (Gligor *et al.*, 2019), it also improves SCRES (Aslam *et al.*, 2020). As a result, it reduces the time required to mitigate risks and their impact (Blome *et al.*, 2013). An agile SC possesses characteristics such as velocity, which enables quick reactions to unexpected changes (Christopher and Peck, 2004; Jüttner and Maklan, 2011). These practices facilitate reducing disruptions' impact on SCs, increasing the SC's ability to respond. SC flexibility and SCRES are positively related (Chunsheng *et al.*, 2020); they allow quick adaptation to disruptions and changes and improve operational efficiency under normal conditions (Pettit *et al.*, 2013). Maintaining an excess capacity to respond to SC disruptions through capital investments requires redundancy (Rice and Caniato, 2003). Building redundancy improves the ability to adapt to disruptions by using excess capacities in production, transportation, inventory and storage facilities (Ali *et al.*, 2017).

Supply chain resilience transforming activities

The third microfoundation of DC theory, transforming, is related to the alignment and realignment of resources and competencies to ensure a strategic fit with sensed and seized risks (Teece, 2007). Essential in dynamic environments, these transformative capabilities induce alterations in existing processes and might be embedded within the parameters of SC reconfiguration and adaptability in SCM. Transforming allows SCs to change their internal processes when needed and continuously improve SC processes, enabling SC partners to learn and co-specialize. By combining integrated sensing and seizing capabilities, firms can identify and exploit emerging short- and medium-term risks. However, transforming requires strategic actions to deal with long-term changes.

Within SCRES, the capabilities that enable SCs to transform may be associated with SC reconfiguration and adaptability. SC reconfiguration relates to adjusting an asset structure and implementing essential internal and external transformations (Teece *et al.*, 1997). SC reconfiguration (Blackhurst *et al.*, 2005; Al Naimi *et al.*, 2021), resource reconfiguration (Ambulkar *et al.*, 2015; Queiroz *et al.*, 2021) and resource mobilization (Pettit *et al.*, 2013) are the main activities that enable resilience in the SC context. While SC agility is concerned with short-term changes and is, therefore, part of seizing, SC adaptability is related to long-term changes through restructuring the SC (Aslam *et al.*, 2018) and is defined as the ability of the firm to change its SC design. This approach is a more radical and long-term strategy compared to changes made to SC agility in response to risks.

In this study, DC theory provides a framework for understanding how SCs can adapt and build resilience in response to rapidly changing business environments (Teece, 2007). This framework is particularly relevant in the context of cyber risks, which are constantly evolving and require businesses to adapt quickly. In addition, this theory provides a lens to examine how SCs manage complexity and uncertainty in their environments, which is particularly relevant in the context of cyber risks (Teece *et al.*, 2016). Furthermore, this theory emphasizes the ability of firms to reconfigure resources in response to environmental changes (Helfat and Peteraf, 2009), which provides a useful perspective on how firms can adjust their resources and strategies to manage SC cyber risks better. These insights allow us to ask the following research question:

RQ1. How can SCs sense and respond to cyber risks to facilitate SCRES?

Methods

In line with the exploratory aim of the study, a multicase study approach was used to facilitate a thorough examination of the research question (Voss *et al.*, 2016). The main objective was to construct a theoretical framework surrounding the concept of SCRES, with a specific focus on cyber risk. While the current body of literature on SCRES and DC is expanding, both have provided a preliminary model for this study; the intention was to extend existing theory rather than create an entirely new theoretical perspective. Consequently, the case study approach used in this research can be characterized as theory elaboration (Ketokivi and Choi, 2014).

In addition, the case study approach is well suited for examining real-world situations in depth, which can be particularly useful for studying complex and dynamic phenomena such as SCCR (Eisenhardt, 2021; Voss *et al.*, 2016). It allows researchers to examine phenomena from multiple perspectives, which is especially important for managing cyber risks in SC. Furthermore, case studies are suitable because they enable researchers to collect data from many sources and create a theoretical model of managers' views and behaviors. Moreover, the selected approach facilitates the elaboration of theories (Ketokivi and Choi, 2014; Fisher and Aguinis, 2017) and theoretical debates surrounding SCRES in the context of cyber risks. Therefore, we used this approach to understand managers' views of and responses to SC cyber risks and their approaches for building SCCR.

Case selection

Initially, four manufacturing firms from various industries were chosen for this research, each operating globally, with headquarters in Central Europe. Using different industries with comparable SC structures enables the identification of differences and similarities. Based on theoretical considerations, the authors then chose 24 industry SC partners from these four initial firms (Eisenhardt and Graebner, 2007). However, the interview and company samples were not predetermined. These firms and their SCs are relevant for developing SCRES to cyber risks, as they are global market leaders in their respective industries. They are actively involved in digitizing their businesses and SCs, and they are suppliers to sensitive industries or critical infrastructure, or they operate in an industry that prioritizes the digitalization of key products. In addition, all four focal firms have recently experienced multiple cyber attacks in their SC. Therefore, the cases representing four firms, including their multilevel SCs as four SCs with at least triadic relations (at least three tiers, in one case four tiers), were carefully selected based on the likelihood of SCCR to occur, allowing theory to be improved based on the similarities and differences of the cases (Eisenhardt, 2021). Furthermore, following the work of Flyvbjerg (2006), we argue that the deliberate selection of cases based on their likelihood of exhibiting SCCR allows for a detailed examination of the conditions under which resilience strategies are most effective. This comparative analysis not only enriches our theoretical framework but also provides a direct link between our empirical findings and the study's research objectives, enhancing the understanding of how different SC configurations influence resilience and risk management practices.

Data collection

A semistructured interview protocol (see Appendix 1) was created to guide the interviews during the data collection process. Between April 2020 and July 2021, the first author conducted 79 interviews from the 28 firms in the four SCs with 59 individuals who worked in roles related to SCM, IT, IT security, purchasing, sales, product management and process management. Participants were selected on the basis of their professional roles, as SCCR is closely linked to their respective roles and experiences. All interviews were recorded, professionally transcribed and then coded by a team of researchers. Due to the COVID-19 pandemic, most interviews (about 95%) took place online using Microsoft Teams. The interview process was repeated until a point of theoretical saturation, based on a diverse range of opinions and in light of the emerging concepts and themes from the data (Gioia *et al.*, 2013). The interviews were open-ended and exploratory, lasting 25–165 min. The authors obtained additional data for the data analysis phase, including material given by the organizations, industry journals and reports and secondary sources of information. Table 1 provides an overview of the SCs, companies and interviewees involved in this study. The information in Table 1, combined with the information in Tables 2, 3 and 4 (which provides details of the interviewee for each quote), allows the reader to identify the chain of evidence. We used specific labels to identify which quotes are attributable to which participant, ensuring a clear link to the respective company and SC.

Data analysis

The data analysis was conducted by a team of researchers, including the authors. For theory elaboration purposes, the case study data were analyzed guided by the theoretical framework (Eisenhardt, 1989; Eisenhardt and Graebner, 2007; Eisenhardt, 2021). MAXQDA, a well-established computer-assisted qualitative data analysis tool, was used to evaluate the interview transcripts. The authors used additional data sources to confirm and explain statements made during the interviews and called all participants again for clarification and feedback. In addition, the transcript, results and analysis were sent, presented to and discussed with the participants to guarantee their accuracy (Lincoln and Guba, 1985; Yin, 2014).

The data analysis process comprises three phases. The researchers began by coding the transcripts *in vivo* (Miles *et al.*, 2020) to gain a better understanding of the data and uncover emergent patterns. The second phase involved the inductive development of open codes. The next stage used further inductive reasoning to condense the open codes into focused codes. Finally, data collection and analysis were carried out until theoretical saturation was attained. Trustworthiness criteria acceptable for qualitative research approaches were used in this study to ensure data collection and processing quality (Hirschman, 1986; Mollenkopf *et al.*, 2011; Russo *et al.*, 2021). Appendix 2 illustrates the trustworthiness criteria underlying this study.

Additional methodological aspects

Before presenting the findings for the three microfoundations of DC, the nature of cyber risks in SCs should be emphasized. It is crucial for this study and the interviews to first create an understanding of cyber risks and their potential impact on SCs. The majority of SC disruptions caused by cyber risks and experienced by participants affect only the availability of products and services. However, there are examples of cyber incidents compromising the integrity and confidentiality of SC assets, which have received little attention in practice and academia.

In this context, it is crucial to establish a common understanding between the interviewer and the interviewees at the beginning of the interview. The conversation should not only focus on the availability of goods and services, as this would equate cyber risks with the conventional risks mentioned in the literature. In addition, the authors want to emphasize that although most case firms have a high level of cyber security

Table 1 Case participants and interview details

Cases	Company (Confidential alias)	Participants and firm profile Firm profile	Business function (Number of interviewees per department)
Case 1: SteSC	Customer SteSC1	Producer industrial supplies	Purchasing (1)
	Customer SteSC2	Producer industrial supplies	Sales (1)
	Customer SteSC3	Producer industrial supplies	SCM (1)
	Customer SteSC4	Mechanical engineering	Purchasing (1)
	SteCo	Technology group	Purchasing (4), IT security (3), SCM (1), IT (1), Sales (1)
	Supplier SteSC1	Industrial supplies	SCM (1)
	Supplier SteSC2	Media technology	CEO (1)
	Supplier SteSC3	Provider of digital services	CEO (1)
Case 2: CriSC	Customer CriSC1	Critical infrastructure	IT security (2)
	Customer CriSC2	Critical infrastructure	IT security (1)
	CriCo	Supplier critical infrastructure	SCM (1), IT security (1), product management (1)
	Supplier CriSC1	Electronic manufacturing service provider	IT (1), sales (1), purchasing (1), quality management (1)
	Subsupplier CriSC1	Board manufacturer	CEO (2)
	Subsupplier CriSC2	Equipment manufacturer	Sales (1), purchasing (1)
Case 3: InsSC	Customer InsSC1	Logistics solution provider	Logistics (1)
	Customer InsSC2	Producer industrial supplies	Purchasing (1)
	Customer InsSC3	Industrial manufacturer	Purchasing (1)
	InsCo	Industrial automation producer	SCM (2), purchasing (2), IT (1), process management (2)
	Supplier InsSC1	Industrial automation producer	CEO (1), sales (1)
	Supplier InsSC2	Producer industrial supplies	Sales (1)
	Supplier InsSC3	Industrial automation producer	Sales (1)
	Supplier InsSC4	Logistics service provider	SCM (1)
Case 4: ComSC	Customer ComSC1	Construction industry	Purchasing (1)
	Customer ComSC2	Construction industry	Digitalization (1)
	Customer ComSC3	Construction industry	Purchasing (1)
	ComCo	Construction machinery manufacturer	CEO (1), SCM (1), logistics (1), IT security (1), quality management (1), product management (1), purchasing (1)
	Supplier ComSC1	Logistics service provider	IT Security (1)
	Supplier ComSC2	Producer industrial supplies	IT Security (2)

Source: Authors' own work

maturity, their understanding of SC cyber risks outside the IT or IT security departments is relatively weak. In all participating companies, almost no executive outside these departments considered or managed cyber threats or risks as part of their job responsibilities. This narrow perspective is mainly due to a lack of awareness, understanding, knowledge, experience and training about cyber risks, as the interviewees reflect. InsCo-SCM-2 expresses the difficulties in understanding cyber risks by stating:

> If you do not really deal with it intensively, and I personally am probably missing it somewhere in my education or have never dealt with it or do not know, it could have 'such and such' an effect. How does the whole thing happen? What happens behind it? I have to say honestly that I cannot grasp it.

The SC understanding and definition underlying this study are broad; they encompass all key SC partners, not simply IT service providers or the digital SC. This comprehensive view enabled the authors to identify disparities in the maturity of cyber risk-relevant SC operations in different departments. While most case organizations had a high maturity level for handling cyber risks in IT-related SC, the study indicates that operational technology (OT)-related or commodity SCs do not. As SteCo-IT-Security-1 explained, "IT could have a problem with the supplier but not the OT. The more digitalized the OT is, the greater the cyber risks there are." Although the share of smart products in raw material SCs has increased in recent decades, all cases show a low maturity level for cyber risk-related SC activities. The main reason for this distinction is that most cyber security standards, such as the International Organization for Standardization (ISO) 27001 or the Trusted Information Security Assessment Exchange (TISAX) in the automotive sector, are focused on IT-related aspects of the SC rather than taking a holistic SC view. This study examines 28 companies within four European industrial SCs that have

Supply Chain Management: An International Journal
Volume 29 · Number 7 · 2024 · 28–50

Table 2 Representative quotes underlying second-order *sensing* themes

Second-order theme First-order concepts	Representative quotes
Sensing	
Creating SC cyber risk knowledge	"Audit accordingly beforehand and see what measures he has, what plans he has prepared for just such an eventuality. Does he have the appropriate safeguards, does he have the know-how or the personnel, or perhaps also a service provider who can help him if something like this should happen, so that he can get back on his feet more quickly?" CriCo-IT-Security "And that is what you can find out during the audit because at least you know what you have, how you are positioned, how the supplier is positioned." CriCo-IT-Security "In our environment, I mainly use service A to take suppliers into such a monitoring system." CriSC1-IT-Security-2 "You need a special monitoring system to find out, but I am convinced that you will find out about blatant issues." ComCo-Logistics "There are also penetration tests. The customer organizes these, or we organize them for the customer." Supplier-SteSC3-CEO "Our customers drive us in the first place. So, we decided very early on that we would like to be certified." CriCo-IT-Security "Our [computer emergency response team] CERT is also looking at the whole issue of situation awareness." Customer-CriSC1-IT-Security-2
Increasing cyber risk-related SC visibility	"Well, these are at the end of the day, we see everything we also have, if it is larger customers corresponding network couplings, the most diverse categories, there is a corresponding network intrusion detection and so on. There is everything you need to implement appropriate visibility and protection." Supplier-ComSC2-IT-Security-2 "Of course, it would be desirable to have end-to-end visibility. But this is hardly possible in terms of effort alone, with the currently available possibilities." Customer-CriSC1-IT-Security-2 "Everything you need to implement is visibility for protection. If you have not implemented anything, you have to react somehow." Supplier-ComSC2-IT-Security-1
Creating SC cyber threat intelligence	"Of course, we also tap into various channels for this. Of course, we have our entire landscape permanently in place for vulnerability management. We scan them, and that is how we get the picture. And another channel is, of course, at least with the large suppliers with whom we have regular exchanges, where the topic is, of course, always whether there are still many risks to be reported from their point of view." Customer-CriSC1-IT-Security-2 "Our colleagues from CERT have outsourced some security services, such as vulnerability scanning, to a partner." Customer-CriSC1-IT-Security-2 "Specialist knowledge or on general data that some market researchers provide." ComCo-Logistics "Our industry CERT and other CERTs also give us the information regularly. It is really almost like the threat intelligence feeds, even if they are almost a light version, but still." Customer-CriSC2-IT-Security

Source: Authors' own work

experienced multiple cyber attacks impacting their SC during the project. All cyber attacks had a detrimental impact on the availability of assets, cascading effects on consumers and suppliers, affecting the flow of products, services, information or finance. However, neither the confidentiality nor the integrity of the assets was compromised, as the incidents only affected SC asset availability.

Findings

A brief overview of the four cases is included in Appendix 3. The findings of the within-case and cross-case analysis suggest that a significant step in building SCRES to cyber risks involves developing a deep understanding of cyber risks and their potential disruptions – labeled as sensing. Thus, the next section discusses how SCs sense cyber threats. Then, it follows a description of how the SCs studied seizing cyber threats and risks and transforming. Together, all three microfoundations are argued to be important for building SCRES to cyber risks. Tables 2 to 4 summarize key constructs from the empirical evidence that serve as the foundation for discussing the three subsections below, and Figure 1 visualizes the data structure of the findings.

Sensing supply chain cyber threats

Sensing refers to SC activities that include scanning and monitoring the operating environment to identify SC cyber threats and risks and make strategic decisions about them. This study identified three specific SCCR capabilities that facilitate the recognition of SC cyber risks: (1) Creating SC cyber risk knowledge; (2) increasing cyber risk-related SC visibility; and (3) creating SC cyber threat intelligence. The following subsections will comprehensively detail the three microfoundations that constitute the sensing capabilities supporting the detection and understanding of cyber risks in SCs. Table 2 summarizes the key constructs derived from empirical evidence that underlie these identified sensing capabilities. Using these capabilities, organizations can strengthen their cyber resilience against cyber

Table 3 Representative quotes underlying second-order *seizing* themes

Second-order theme First-order concepts	Representative quotes
Seizing	
Prioritizing short-term cyber risk-related SC collaboration	"Exactly this whole topic also plays a role in customer discussions. Then it is usually the case that our customers also ask us, have you looked at this, what is the status of this and then they ask for information." Supplier ComSC2 "Have clear and end-to-end risk management, also in terms of failures of any kind of the sourcing sources and risk management operations, look at and accordingly have failure scenarios. Especially with such single-source things and with such important raw materials." InsCo-SCM-1 "We have to make a risk assessment for each supplier if there are any risks that could arise, so that we can make appropriate arrangements with the supplier." CriCo-Product-Management "Yes, I think the challenge is, in terms of the new approach, to develop further from the classic risk management, concerning common knowledge of the damage event, from which damage is to be foreseen. I think that is where you reach an agreement, through communication, through confidential communication, to get that information. But just this one, so as not to be flooded by too much information. I think that this is the new discipline that has to emerge. Between 0 and 1, risk management and non-delivery must happen." SteCo-IT-Security-1 "We have to weld our IT department together with that of the supplier, so that we naturally try to achieve some kind of information exchange as quickly as possible. That, I would say, is the link that we would make there." Customer-InsSC2-Purchsing
Building cyber risk-related SC flexibility	"The advantage of our SC is the flexibility in finding a task force across divisions that quickly takes care of such problems." InsCo-SCM 1 "The homepage was down, and the customers were informed relatively quickly on the homepage that we had been hacked." Supplier-InsSC1-CEO "And I was primarily responsible for communication with customers and employees. So, that was my role, and I just tried to create awareness among the team quickly. That means, of course, that was a challenge. How to get the right information to everyone on short notice. Because there are no emails, not everyone has a telephone, field staff has a telephone, and office staff does not have a telephone. First, it was very challenging to find a channel to reach everybody. That was one of the main things we did at the very beginning." Supplier-InsSC1-CEO "That is, we first, of course, communicated with the customers, informed the field staff, who then also had contact with the most important customers via their cell phones. Everyone was encouraged to communicate quickly and to create an understanding of the delays among the partners." Supplier-InsSC1-Sales "Yes, to a certain extent, to prepare something like that perfectly, that is, of course, difficult. I think we had to work agilely there as well. And there were contingency plans and scenarios, but that you can do that down to every detail – you realize how it really is when it is there, that is why, such a mixture, I would say. Today, of course, on a completely different level, so we know immediately what we are doing and how." Supplier-InsSC1-Sales
Building SC cyber risk culture	"Our CERT is also looking at the whole issue of situation awareness." Customer-CriSC1-IT-Security-2 "If, for example, one of our partners is attacked, they inform us, and this then goes straight to our cyber security. And then from there – the steps are initiated; IT is well aware of the scope of the SC." Supplier-InsSC1-Sales "The Cyber Range was officially inaugurated last year. There is no comparable institution in our country. Internationally, there are similar ones. But in general, the difference from some other training facilities is that, for example, the substations are not simulated here, but there is the related technology. So, the secondary technology, primary technology as simulators. But you really have a piece of hardware that is there. And with many other training facilities, it is also the case that this is completely virtualized." Customer-CriSC1-IT-security-1 "If something should happen, and I do not think you can get by without cyber insurance anyway." Customer CriSC2 "We have a cyber security insurance policy, which the parent company holds, but of course applies to the group as a whole, which is the umbrella for everyone." SteCo-IT-Purchasing "This has also led to a rethinking of certain things, for example, the entire data security at our company, when a hacker attack occurs, and we have to press the shutdown button and pull the plug, so that we really only lose five minutes." CriCo-SCM "And simply that one recognizes that – and also really takes into account that there are extreme risks out there. And for me, above all, a soft factor that I feel to this day that is also important is that you have the understanding of the department for each other and together for the customer – this – this has always been anchored in our culture but was never as strongly livable as at this moment, and I think that is still there today." Supplier-InsSC1-Sales

Source: Authors' own work

threats by developing an understanding of potential risks. In addition, by increasing SC visibility and improving SC threat intelligence, they can make informed strategic decisions to respond to such risks and threats.

Creating supply chain cyber risk knowledge

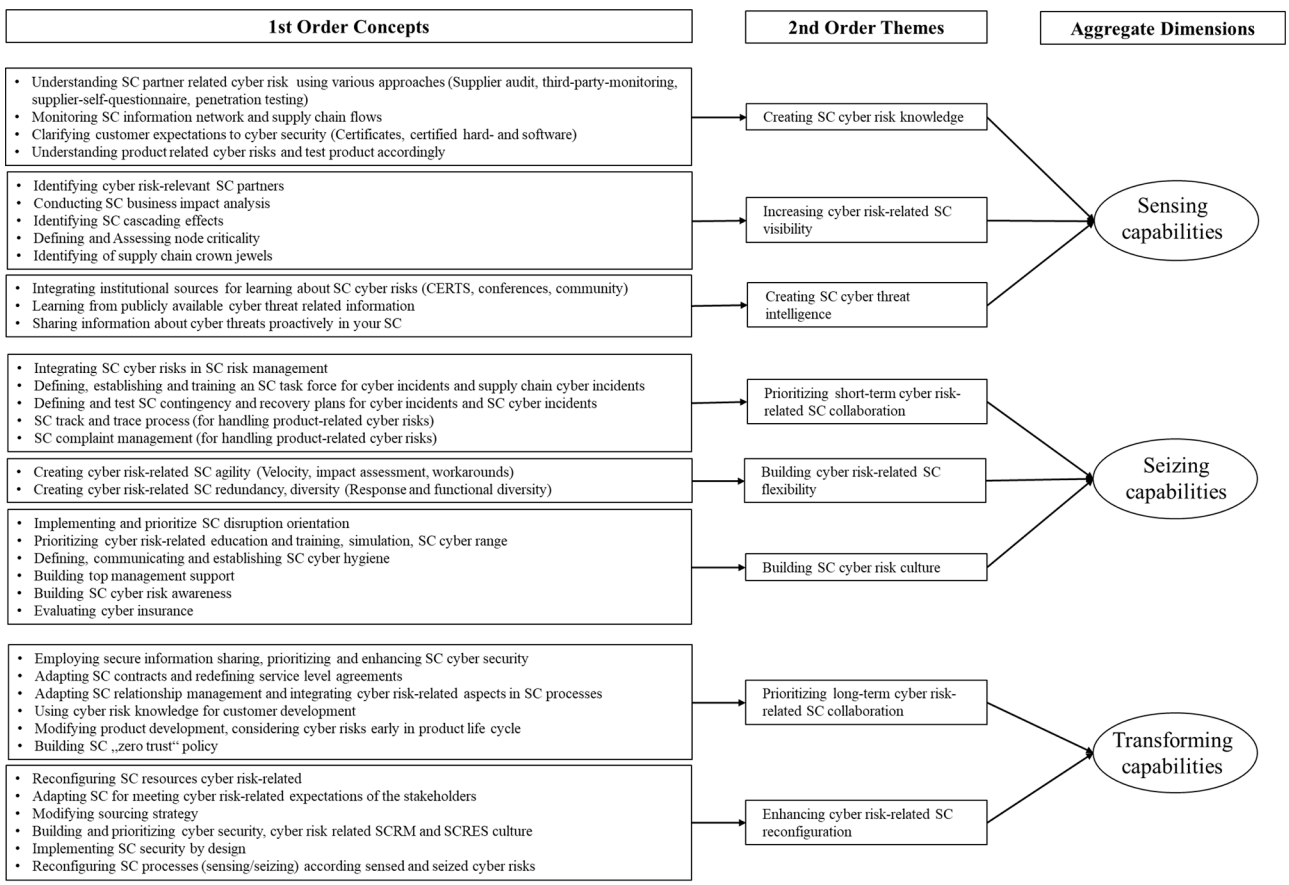
Improving SCCR first requires broadening the awareness and understanding of cyber risks within the SC to enable a nuanced understanding of SC operations in this specific context. For the

Table 4 Representative quotes underlying second-order *transforming* themes

Second-order theme First-order concepts	Representative quotes
Transforming **Prioritizing long-term cyber risk-related SC collaboration**	"Because we have done many things where we realize that we also have a strategic component when we say that the support from the supplier in this process is expandable. We will have other requirements in the future. For example, patching must be faster. The processes must be adapted. Then, you have something that is geared toward the long-term. We will then be in dialogue with the suppliers again. If necessary, there will be an adjustment to the contract. And if this should also have a monetary effect, then, of course, purchasing would be involved again." Customer-CriSC1-IT Security-2 "That is the key, being proactive. That you say, they have to inform much more. In reality, you only get most of the information when they ask for it." Customer-InsSC1-Logistics "That is, we certainly today find faster channels, secure channels to manage." Supplier-InsSC1-Sales
Enhancing cyber risk-related SC reconfiguration	"That is, you have any problems with it all the time, and now they are strategically going to a in the medium-term, for example, so that their software runs under A. Because with B, the whole vulnerability management is already very impracticable in some cases." CriCo-Product-Management "And we have an internal CERT that coordinates all the processes and takes action in the event of incident response. They then call support as needed. We are lucky that we have an internal CERT." Customer-CriSC1-IT Security-2 "In the area of incident response, we have contracts, but then we have on-call contracts. To simply have resources with the necessary know-how available in the event of an incident. Which is usually the main purpose." Customer-CriSC1-IT-Security-2

Source: Authors' own work

Figure 1 SCCR data structure findings based on DC



Source: Authors own work

Supply Chain Management: An International Journal
Volume 29 · Number 7 · 2024 · 28–50

companies studied, cyber risks currently represent only a marginal component of SC operations, indicating a lack of deep-rooted cyber risk awareness and knowledge across multiple entities. Consequently, integrating cyber risk considerations into SC operations is key. This integration will make it easier for companies to learn more about their SC partners, focusing on areas such as self-assessing suppliers through surveys, conducting supplier audits or using third-party monitoring services. SteCo, CriCo and InsCo could take advantage of existing strategies already implemented by their IT departments. These case firms combine various approaches, but Customer-CriSC1-IT Security also sees the use of audits as demanding:

> So, the self-assessment is the basis. And then, we will go on-site if necessary. Depending on the criticality, we are talking about thousands of service providers. If you take them all together, we will certainly not be able to audit them all every year or at very short intervals. But, of course, that is the basis, and then it will be audited on-site; then there will also be another telephone call perhaps to clarify some questions.

Conversely, ComCo needs to develop strategies to address the lack of IT capacity and cyber risk awareness among its SC partners. Currently, audits and self-assessment surveys are only used for a selected group of suppliers, with little consideration given to cyber risks, again indicating a lack of cyber risk awareness and knowledge. Such an approach could be expanded to ensure a comprehensive and effective cyber risk strategy.

The strategic use of these tactics is crucial for current and future suppliers and the corresponding SC at all stages of the product life cycle. The level of SC visibility determines this alignment. Central to this process is the cybersecurity posture of critical SC partners and the flow of products, information and finances to and from all SC partners. An effective scanning and monitoring program for these flows is critical to identifying potential cyber risks. Understanding the unique nuances and inherent cyber threats associated with different SC partners will increase knowledge of the associated risks. Cyber risk considerations should be integrated into product testing procedures and contribute to the knowledge base of cyber risks associated with goods and commodities circulating within SCs.

This integration into the whole product lifecycle is particularly important for CriSC, InsSC and ComSC as they are large-scale producers of smart products. Therefore, it is imperative for SC personnel to proactively monitor potential cyber threats and risks from both supplier and customer perspectives. This includes focusing on potential cascading effects and cross-movement risks. Consequently, fostering capabilities within the SC that facilitate regular identification and assessment of cyber threats and risks is beneficial. By incorporating cyber risk considerations into all SC processes, a more comprehensive understanding and effective management of SC can be achieved. Improved knowledge of cyber threats and risks in the SC enhances context-specific knowledge and helps to identify potential disruptions, as cyber threats can originate from any point within a given SC.

Increasing cyber risk-related supply chain visibility

Improving knowledge about cyber risks among SC partners requires a nuanced perspective on SC visibility that differs from traditional SC risks. Unlike localized threats such as natural disasters, cyber risks have the potential to affect all partners within an end-to-end SC, regardless of geographic location. This widespread vulnerability is due to the complex interplay of the digital network and its vulnerabilities. In addition, the availability, integrity and confidentiality of SC resources can be compromised by combining multiple attacks simultaneously. Given this ubiquity of cyber risks, no partner within an end-to-end SC is exempt. Therefore, comprehensive visibility across the SC may be required to develop an accurate understanding of the current state of the SC.

Given the limited level of visibility in all four SC studied, it is essential to identify key SC partners and expand visibility in response to the identified risks. The cross-case analysis of the SCs studied revealed patterns that underline the need for iterative and continuous assessment. As the CriCo manager from the product management department explained, "If you now look at the topic of cyber security in detail, you have to define the system and which SC partners are part of it. Who is relevant from the cyber risks point of view?" Therefore, the initial steps of detection activities need to be iterative and continuous. In addition, the potential for cascading effects and lateral movement must be considered while increasing visibility beyond first-tier SC partners. This increased visibility facilitates the identification of relevant SCs and the assessment of their current state, which is the basis for identifying the weakest SC links. These may represent SC vulnerabilities in one area that could lead to systemic weaknesses, especially if key partners are not adequately secured. IT capabilities can further extend this visibility and deepen the SC's knowledge of cyber risks.

Creating supply chain cyber threat intelligence

While the first two sensing microfoundations focus mainly on the internal aspects of SCs, the third sensing capability focuses on the integration of external information and activities, which is vital for creating a holistic understanding. For instance, the IT security departments in all four SCs studied typically pursue a strategy of consolidating and disseminating information about cyber risks and vulnerabilities from various sources. These sources include commercial services, computer emergency response teams (CERTs), communities and conferences. Rather than limiting the dissemination of this valuable information to a single company, it is critical to proactively disseminate it throughout the SC or share it with specific SC partners. The first two sensing activities can form the basis for identifying the relevant partners who are critical to effectively sharing cyber threat information in the SC.

Although most SC managers interviewed in the study emphasized the importance of knowledge creation and improved visibility, sharing cyber threat information with SC partners is significantly prevalent, especially in CriSCs. Furthermore, a sophisticated approach to cyber risk activities facilitates the smooth sharing of important information. This is likely due to the fact that this SC has the highest level of maturity in managing cyber risk activities. As the IT security manager of the client CriSC2 explained, the goal is to build SC-focused cyber threat intelligence:

> What we are, of course, already trying to do … is to focus more on threat intelligence, also attack surface management, so that we can find out what is planned against our SC. And we can then react accordingly before an attack occurs. Quite simply, but only on the roadmap for the future.

Supply Chain Management: An International Journal
Volume 29 · Number 7 · 2024 · 28–50

SC cyber threat intelligence is an additional sensing activity that complements the previous two sensing activities by using external threat-related information. In addition, this third capability can be used to share data collected from all seizing activities with SC partners to promote a more unified approach toward SCRES against cyber threats.

Seizing: Activate supply chain resources to address sensed supply chain cyber risks

To address sensed cyber threats and risks, SCs should develop capabilities related to seizing activities. In this study, these capabilities are: (1) prioritizing short-term cyber risk-related SC collaboration; (2) building cyber risk-related SC flexibility; and (3) building SC cyber risk culture. Table 3 summarizes the key constructs from the empirical evidence that serve as the foundation of the identified seizing capabilities.

Prioritizing short-term cyber risk-related supply chain collaboration

After sensing cyber threats and risks in the SC, the key response of the case companies was to work with their SC partners to address these perceived threats and risks. The main difference between SC collaboration in seizing and transforming lies in the time horizons. The former is a short-term strategic response, while the latter is a long-term approach that involves discourse and structural change. A collaborative approach to SC risk management becomes the first process of assistance after a threat is detected. As CriCo's product manager notes:

> We do this via all components that are inside our products, such as hardware and software components. We have such a process. Some of the information channels are the Internet, some are mailing lists where we get the information. Some are agreements with suppliers where they inform us, and they write into the system, where they inform us about vulnerabilities. And we have a ready-made process, who takes care of it, who does the risk assessment, and who then decides, we integrate that into the product.

It is imperative to understand that when a cyber risk is discovered that affects an SC asset such as a product or service, it is of utmost importance to obtain comprehensive information about all elements within the SC that are potentially affected by this vulnerability. Ideally, an SC tracking and tracing process would be quickly initiated to identify these elements throughout the end-to-end SC. However, the focus of this process should not be exclusively on the company's products. CriCo's product manager illustrates the importance of this broader view:

> But in any case, I need a process that says when parts of purchasing or SCM are determined, the supplier has been hacked and in turn. Specifically in my area, so in the product area there are people who are then responsible, who can evaluate whether there are now risks in the delivered products. They can examine the product, test it, and then evaluate whether there is a significant risk or not.

When such vulnerabilities are discovered, it is important to implement an appropriate SC complaint management process, both upstream and downstream, to enable a quick response to these vulnerabilities. The SC complaint management process, thus, complements the SC tracking and tracing process. This iterative approach ensures constant alignment between emerging risks and established structures, streamlining responses. This process is of great importance for managing the flow of products in the SC, especially for dealing with products that do not meet consumer expectations. Cyber attacks have the potential to undermine the integrity of products, with vulnerability potentially emanating from any point within the SC to take advantage of them. On this topic, the quality manager of the supplier CriSC1 shared the following insights:

> The most sensitive thing that can happen is that the customer has a complaint in the process of being resolved, that he says he has some kind of problem, and that we then have to start an analysis with the subcontractor.

To extend this example, a computer chip manufactured in the fourth tier of an SC may result in consumer vulnerability and enable an SC cyber attack that affects thousands of firms and different SC tiers simultaneously.

In the event of an SC disruption due to a cyber attack, it is essential to quickly assemble a task force within the affected company that includes the relevant SC partners. This measure underlines the replication logic in practice, which treats each incident as a unique observation to adjust responses effectively. Speaking about the process of putting together a task force, ComCo's quality manager revealed:

> There is a task force that is always put together depending on the problem. For example, someone from our IT specialists would be asked to come down to the table if it were a cyber issue. That works quite well for us because everything is concentrated at the site. We do have all the departments there. And communication is good. We do not have a lot of siloed work.

Given the potential chaos immediately following a cyber attack, the SC response should be supported by jointly developed and pretested SC recovery plans. While all four SCs agree on these procedures, it is essential to underline the theoretical argument that these SC strategies need to evolve as most of them are currently focused primarily on the focal company only.

Building cyber risk-related supply chain flexibility

SC flexibility in the context of cyber risk has two critical dimensions. The first is SC agility, which is critical to facilitating rapid responses. Swift action is critical once cyber risks or incidents are detected, as it allows for timely mitigation of potential impacts. This requires constant comparison, a rapid iteration between risk detection and response. In addition, rapid information sharing and cyber risk assessment are equally important for assessing the potential impact of disruptions. The sooner an impact assessment is conducted, the sooner decision-makers can take corrective action to mitigate the consequences. Due to the latent nature of cyber risks, which can remain hidden until they impact the SC, SC visibility, supported by cross-case analysis, is paramount to enable a rapid response. In this context, InsCo's SC manager said:

> And then quick decisions are found. Whom do you need, what is the problem, what are the options? And then all the alarm bells start ringing, and within one or two days, it quickly happens that you have a team. One that has a flat hierarchy. One that has also discussed the possibility with the executive committee directly.

The second critical dimension of SC flexibility in relation to cyber risks concerns redundancy and diversity. Redundancy has particular importance in this context. Traditional redundancy in the SC is not necessarily beneficial in the event of cyber incidents. For example, if a supplier operates from multiple locations, this usually increases resilience against disruptions due to natural disasters. However, if a supplier experiences a cyber attack, all of its global locations will probably be impacted simultaneously due to their digital

connectivity. Consequently, it is essential to have redundant procedures in place that allow the supplier to maintain production and delivery of products and services even in the event of a cyber attack, as confirmed by the supplier's sales manager InsSC3:

> And then, very quickly, there is another way in which we can continue to work, and that is the most important thing about it. In the first moment, you only notice that something is not working. Then, all the offline work has largely worked. I got no emails and could not send any. Nevertheless, our enterprise resource planning system, which runs differently, continued to work. So, SC-wise, we were okay. It was just that the communication did not work right away. And I think, within half an hour, we had the bypass, completely set up across all the capabilities.

In the event of a cyber attack that disables everyday means of communication, the immediate establishment of an alternative route for SC communication and information exchange becomes paramount. Therefore, it is necessary to re-evaluate the concepts of redundancy and diversity to recognize each SC entity as a unique observation with its own vulnerabilities. For example, if a company relies on two suppliers for redundancy, but both depend on the same critical IT service provider, the security of the company is at risk. Identifying such cases is central to improving flexibility and highlights the critical role of creating SC knowledge. Assessing SC flexibility in the context of cyber risks is, therefore, essential, as cyber risks have unique characteristics that require special considerations and preparation measures. Furthermore, this approach ensures a comprehensive understanding and not just a description of cyber risk scenarios in the SC.

Building supply chain cyber risk culture

Establishing a cyber risk culture in the SC increases collaboration and flexibility and equips it with the necessary tools to address cyber risks effectively. This study demonstrates that focusing on SC disruption and building a cyber risk management culture can enhance a company's resilience to SC cyber disruptions. The ability to learn lessons from past disruptions is closely linked to the SC's ability to manage future disruptions. Throughout the study period, several participating companies faced cyber attacks. Participants confirmed that the lessons learned and experiences gained during the COVID-19 pandemic were invaluable resources in managing the impact of cyber incidents in their SCs. Conversely, their experiences with the pandemic informed their handling of cyber incidents, emphasizing the universality of foundational crisis management principles across various types of disruptions. CriCo's sales manager shared her experience of using her COVID-19 pandemic response expertise to quickly manage the impact of a cyber attack on her client, SteSC4, despite having no previous experience of dealing with such situations:

> COVID-19 was such a disturbance that I could refer to. There were similar situations. We were not able to estimate exactly when things would continue or when the customers would need material again. It was similar, I must say. That is why COVID-19 was a good exercise to know what my next steps are.

It is critical that staff in all departments involved in the SC, especially those directly involved in cyber risks, are trained to develop awareness of the cyber risks relevant to their respective departments. This need for awareness and training is underlined by the persistent misconception that cyber security is the exclusive domain of the IT department, while other departments remain largely uninformed about the potential cyber risks within their SC activities. Therefore, an all-encompassing, cross-departmental approach to cyber security is of utmost importance. As a result, investing in education, training, simulation exercises and awareness campaigns is critical to creating a robust cyber risk culture. Such a change needs to be supported by top management, as ComCo's IT Security Officer pointed out:

> But you can see that awareness of the issue of security has risen sharply in recent years, even among top management. And also, the awareness that, as a company, you tend to work in a partner network with many, many partners. Rather than still doing everything on your own and only relying on yourself.

In broadening the scope, this study revealed a discrepancy in awareness: While cybersecurity managers generally recognize the importance of considering the SC, many SC managers largely overlook the cyber risks associated with their operations. This lack of awareness is not limited to SC managers but extends to all departments involved in SC operations and includes areas such as sales and product development. This research described three key microfoundations for effectively seizing identified cyber risks in SCs: (1) Prioritizing short-term cyber risk-related SC collaboration; (2) building cyber risk-related SC flexibility; and (3) building SC cyber risk culture. These elements complement each other and form the structural and practical basis for SCs that are equipped to deal with identified cyber risks. Taken together, these aspects, when harmoniously integrated, form a robust framework that enables SCs to navigate the turbulent seas of cyber threats with resilience.

Transforming: Aligning supply chain resources and capabilities

SCs need to proactively and strategically manage their internal and external competencies, routines and resources to renew existing routines and address cyber risks. The essential capabilities required to transform and reconfigure are: (1) Prioritizing long-term cyber risk-related SC collaboration and (2) enhancing cyber risk-related SC reconfiguration. The first capability aims at long-term improvements by leveraging identified and captured cyber risks within existing SC partnerships. In contrast, the second capability aims to change SC design and substitute existing SC partners. Table 4 summarizes the key constructs from the empirical evidence that form the basis for the identified transforming capabilities.

Prioritizing long-term cyber risk-related supply chain collaboration

The dichotomy of SC collaboration between seizing and transforming microfoundations lies in their temporal focuses. While the former is primarily concerned with immediate adjustments, the latter is oriented toward long-term aspects. Although cyber risks are a significant concern for most case companies, the severity of these risks experienced by the case companies did not require SC reconfiguration across all companies due to limited impacts, mainly on the availability of SC assets. The study's findings suggest that companies need to cultivate a strategic, long-term collaboration with SC partners to initiate transformative change. Such change requires extensive coordination and realignment of various processes, resources and capabilities to address cyber risks and build

SCCR comprehensively. An example of this strategy was provided by the sales manager of Supplier-InsSC1, who reported on the changes initiated after a cyber attack:

> SC data, such as communication, we have newly established a whole department, we also had one person taking care of it before, but now there is a whole staff attached to it. This means, of course, that professionalism has now been raised to another level. Before that, we had one person who was responsible. A team expanded this person. We have worked a lot with external people who also advised us. But now we have a permanent department, a small group, which has the whole store in view, as far as the topic is concerned. They always need to be notified when something happens around us. They certainly have a concept that addresses the environment and our partners.

Establishing dedicated units or teams indicates a proactive stance to cyber risks. Such forward-looking approaches underscore the recognition that cyber threats are an ongoing, evolving challenge that warrants consistent attention rather than sporadic responses. It also signals the company's commitment to protecting its SC from potential cyber disruptions, fostering trust among partners and demonstrating a willingness to adapt and evolve in an increasingly digital landscape.

Enhancing cyber risk-related supply chain reconfiguration

While SC collaboration emerges as the preferred capability for transforming, the current study emphasizes the need for SC reconfiguration when existing arrangements prove insufficient to strengthen SCCR. This perspective is evident in the comments of CriCo's IT security manager, who states:

> If the supplier does not adhere to the IT security specifications, for example. So, if we have agreed on certain rules, how he must keep or protect his data, or how he must perform services as we do, he does not adhere to them. And we communicate that with him, and he still does not do that. So, as I said, we were on the verge of kicking someone out anyway.

Such a determined stance underscores the centrality of cyber risk management in today's digitalized business landscape.

Given the specialized nature of cyber risk-related activities, they often require expertise that SC managers may lack but can easily be provided by other internal departments, such as IT, IT security or CERT. By merging SCM and cybersecurity expertise, companies can develop a holistic approach that effectively combats potential cyber vulnerabilities and threats. Therefore, organizing cyber risk-related SC activities in collaboration with internal and external cyber security experts is crucial for building SCCR.

In this study, we find that procurement strategies may need to be reconfigured when cyber risk considerations take a key position alongside other established criteria such as price and quality. This shift underscores the growing importance of cybersecurity in contemporary SCM. It suggests that price competitiveness and product quality alone can no longer be the only determinants of SC partnerships. Therefore, it is critical to implement a recurring process to reconfigure SC processes identified in sensing and seizing to manage cyber risks effectively. In light of these findings, there is a need to establish a cyclical process whereby the SC processes identified in the detection and capture phase are periodically reviewed and, if necessary, reconfigured. Such recurring assessments will ensure that the SC remains agile, adaptable and adequately equipped to proactively address the ever-changing cyber risk landscape.

Discussion

While existing literature discusses SCRES and DCs, our study specifically explores these concepts in the context of cyber risks, a relatively underexplored area. The study proposes the novel idea of integrating general SCRES capabilities with specific SSCR capabilities. By offering an in-depth understanding of how the three clusters of DCs (sensing, seizing and reconfiguring) apply to managing cyber risks in SCs, our study expands upon the existing body of knowledge on DCs. The study shows that SCRES to cyber risks depends on how effectively the SC coordinates complementary resources and competencies around a dynamic and vulnerable environment that includes cyber risks (Pandey *et al.*, 2020). Therefore, SCs need organizational and managerial SSCR capabilities that form the basis of three distinct clusters of DC. Teece *et al.* (1997) argued that DCs are organizational and managerial capabilities that enable firms to address risks outside their daily routines. To address SC cyber risks, combining general SCRES capabilities with specific SCCR capabilities is essential. Furthermore, the study shows that DCs help SCs invest in their ability to address cyber risks. These empirical findings allow us to introduce the following proposition:

P1. A combination of SCRES and specific SCCR capabilities supports cyber risk-related SC processes of sensing, seizing and transforming to increase SCCR.

Our research extends the understanding of SC cyber risks within the broader context of SC risks by delineating their unique characteristics. Cyber risks pose a triple-threat to the confidentiality, availability and integrity of SC assets, which can significantly intensify SC disruptions. In addition, SC assets could already be at risk through infiltration that is not discovered throughout the SC. Cyber risks may remain undetected for a long time before impacting the SC. The longer the duration, the more significant the potential impact and cascading effects on SCs. These aspects distinguish them significantly from traditional threats and complement specific findings from previous SCRES literature (Alvarenga *et al.*, 2023; Gaudenzi *et al.*, 2023; Holgado and Niess, 2023; Yaroson *et al.*, 2021).

We uncover a critical gap in the interaction between SC managers and IT security professionals, underlining the need for unique cybersecurity measures within traditional resilience models. This substantiates the work of Creazza *et al.* (2022), who emphasized the importance of management awareness in navigating the cyber threat landscape. Accordingly, our findings propose that a focused orientation toward cyber threats enhances SCCR. This proposition not only reaffirms but extends Walker's (2020) work by emphasizing the role of threat-specific resilience measures. As such, our research presents a novel contribution by asserting that SC orientation toward cyber threats and risks is imperative for improving SCCR. This leads to the following proposition:

P2. An SC-focused orientation toward recognizing and managing cyber threats and risks enhances its cyber resilience.

Supply chain cyber risk-related sensing capabilities

The present research emphasizes that the foundation of building SCCR lies in fostering awareness and generating

extensive knowledge regarding the specific nature and potential implications of cyber risks in the SC. Given the inherent complexity and far-reaching implications of cyber risks, which may potentially impact all partners and assets across the SC, this knowledge creation process presents unique challenges that stand apart from the acquisition of information pertaining to conventional SC risks, as delineated in the existing literature (Ali *et al.*, 2023, Scholten *et al.*, 2019).

This study, therefore, not only substantiates the existing body of SCRES research, that knowledge creation serves as a cornerstone of strengthening SCRES (Scholten and Schilder, 2015; Umar *et al.*, 2021), but further elucidates the necessity of acquiring specialized knowledge about SC cyber risks. This is a novel contribution as this specific facet of knowledge creation is seldom addressed in the existing literature. The research findings emphasize the importance of including specific information about cyber threats and risks and their potential impacts in SC knowledge creation to enhance SCCR. The empirical findings allow the introduction of the following proposition:

P3. Enriching SC knowledge with specific insights into cyber threats and risks improves sensing capabilities critical for building SCCR.

The research underscores that, as SC visibility enhances SCRES in general (Scholten and Schilder, 2015; Mubarik *et al.*, 2021), it becomes crucial to increase SC visibility to generate knowledge about SC cyber risks. This is particularly important considering the widespread cascading effects and lateral movement characteristic of cyber risks. Colicchia *et al.* (2019) highlighted visibility's role in managing cyber risks, and it is a necessary condition for responding to risks, which is thereby critical for SCRES (Pettit *et al.*, 2010). Moreover, the potential of SC visibility in mitigating cascading effects and lateral movements that characterize cyber risks extends the traditional scope of visibility's contribution, as identified by Melnyk *et al.* (2022).

These findings extend the existing understanding of SC visibility in SCRES building by elucidating its amplified importance in the context of SC cyber risks. While previous literature underscored visibility's role in enhancing general SCRES, this study reveals its more pronounced role in managing cyber risks. Moreover, visibility's potential in mitigating the characteristic cascading effects and lateral movements of cyber risks extends the traditional scope of visibility's contribution. Thus, the study deepens the discourse on SC visibility, highlighting its significant role in sensing capabilities for building SCCR, a novel contribution to the existing body of knowledge, which leads to the following proposition:

P4. SC visibility, specifically considering SC cyber threats and risks, positively impacts sensing capabilities for building SCCR.

The study underlines that while mutual understanding and knowledge generation along the SC is essential, the unique challenges posed by cyber risks demand more proactive measures. Namely, it is crucial to integrate and distribute external cyber risk-related information and to share it proactively with SC partners. The necessity for this level of information sharing is underscored by the fact that a wealth of publicly accessible information regarding cyber risks exists, and any of these risks could pose a potential threat anywhere along the SC.

This finding not only reinforces but further expands the discussion of Colicchia *et al.* (2019) regarding sharing knowledge through threat intelligence. It moves the conversation from a broad consideration of knowledge sharing to a more focused exploration of sharing cyber risk-related information specifically. Furthermore, the study aligns with previous work, recognizing that resilience to cyber risks in the SC improves through knowledge sharing across the SC (Radanliev *et al.*, 2020). This is especially true for cooperation with small- and medium-sized enterprises (Bak *et al.*, 2020). However, what sets this study apart is its emphasis on integrating external cyber threat information and its proactive dissemination amongst SC partners. This notion is relatively unexplored in the current literature. Therefore, this research offers a unique insight into the nuances of information sharing in building SCCR. This leads to the introduction of the following proposition:

P5. SC activities that specifically integrate external cyber threat information and proactively share it with SC partners improve sensing capabilities for building SCCR.

Supply chain cyber risk-related seizing capabilities

Our research uncovers that proactive SC collaboration is fundamental in building seizing capabilities, indicating that firms should collaboratively manage detected cyber risks within the SC. Our findings, built on previous resilience research that identified SC collaboration as a key strategy for addressing SC risks (Scholten and Schilder, 2015; Scholten *et al.*, 2019; Tran *et al.*, 2016), bring new emphasis to its role, specifically in addressing cyber risks. We further propose integrating track-and-trace processes and complaint procedures concerning upstream and downstream SC partners throughout the product lifecycle. Our work aligns with recent insights from Colicchia *et al.* (2019) and Ghadge *et al.* (2019) on the effectiveness of SC risk management in bolstering SCRES to cyber risks. In addition, we emphasize the efficiency of task forces and recovery plans, particularly during the postdisruption phase (Creazza *et al.*, 2022). These unique additions to the existing body of knowledge create a compelling new perspective in understanding the complexities of building seizing capabilities for SCCR. Therefore, we propose that proactive SC collaboration to address sensed cyber threats and risks improves seizing capabilities for building SCCR. This discussion leads to the following proposition:

P6. Proactive SC collaboration to address sensed cyber threats and risks improves seizing capabilities for building SCCR.

Building on the existing body of work (Gligor *et al.*, 2019; Aslam *et al.*, 2020; Chunsheng *et al.*, 2020), our research further accentuates the criticality of SC flexibility, agility and redundancy, specifically in the realm of cyber risks. We posit that, in the face of cyber threats, these capabilities need to be fine-tuned and implemented to enhance SCCR effectively. Our findings elucidate how response diversity and functional

diversity emerge as key strategies for addressing sensed cyber risks, mainly due to the pervasive disruptions they can inflict. While the previous work by Ghadge *et al.* (2019) and Melnyk *et al.* (2022) underscored the role of SC flexibility in managing cyber risks, the specific context of cyber risks was not elaborately discussed. By placing these capabilities within the unique context of cyber risk, we contribute a novel perspective to the discourse. Based on this, the following proposition is suggested:

P7. Cyber risk-related SC response and functional diversity support SC flexibility and increase seizing capabilities for building SCCR.

This study accentuates the importance of fostering a culture that perceives cyber risks as a holistic SC issue rather than a standalone departmental responsibility. Our findings converge with previous research emphasizing the role of SC orientation and SC risk management culture (Chowdhury and Quaddus, 2016) and the significance of shared norms and common culture in mitigating cyber risks (Colicchia *et al.*, 2019). In addition, acknowledging cyber security as an overarching SC issue (Melnyk *et al.*, 2022) resonates with our findings. Despite SC awareness being widely recognized in SCRES literature as a sensing activity (Datta *et al.*, 2007; Sáenz and Revilla, 2014), our study underscores that cyber risk awareness is more pivotal as a seizing activity. We argue that this stems from the observation that while managers are generally aware of cyber risks, these threats are not always integrated into their work environment. Consequently, cultivating an SC cyber risk culture can support practitioners. This leads to the following proposition:

P8. SC cyber risk culture positively contributes to seizing capabilities for building SCCR.

Supply chain cyber risk-related transforming capabilities

The empirical evidence from this study underscores the pivotal role of sustained SC collaboration in tackling immediate and long-term cyber risks. This observation is consistent with the previous literature that emphasized the necessity of resource transformation for improving SCRES against various threats (Blackhurst *et al.*, 2005; Ambulkar *et al.*, 2015; Al Naimi *et al.*, 2021). The proactive alignment and transformation of SC resources and capabilities through sustained collaboration heralds a strategic shift from merely responding to risks toward anticipating, and, thus, more effectively mitigating, potential cyber threats in the SC. While Ghadge *et al.* (2019), Creazza *et al.* (2022) and Melnyk *et al.* (2022) have focused on managing cyber risks in SCs, our work delves into the details of resource transformation within the specific context of cyber risks. Therefore, the insights yielded from this study add new dimensions to our understanding of SCCR, emphasizing the importance of long-term collaboration and strategic resource transformation in enhancing it. Based on this discussion, the following proposition is suggested:

P9. SC long-term collaboration for aligning SC resources and capabilities to address SC cyber threats and risks improves transforming capabilities for building SCCR.

The empirical findings of this study underscore the inherent role of trust and collaboration in today's SC dynamics, emphasizing the need for strategic SC reconfiguration rather than just reactionary changes to enhance SCCR. This perspective complements existing literature on SCRES, which traditionally focuses on adjusting existing resources and capabilities to respond to risks (Ambulkar *et al.*, 2015; Pettit *et al.*, 2010). The reality of contemporary SCs, with complex and evolving cyber risks, necessitates a more proactive, transformative approach to managing such threats. SC managers often lack specific knowledge about cyber risks. Therefore, it is essential to incorporate external expertise into the SC and forge novel resource combinations. This entails the necessity of a long-term vision for SC cyber risk culture that supports innovative resource reconfigurations and integrates the criterion of cyber risk into the decision-making process. Moreover, to fulfill the requirements of sensed and seized SC cyber risks, there is a need to rethink the SC design itself. This includes integrating new SC partners that align with the imperative of cyber risk management and, where necessary, replacing existing partners who may not fit this new paradigm. Consequently, the findings of this study expand upon previous literature by highlighting the importance of a holistic reconfiguration of the SC in the face of cyber threats and risks. This leads to the following proposition:

P10. SC reconfiguration to address sensed and seized cyber threats and risks improves transforming capabilities for building SCCR.

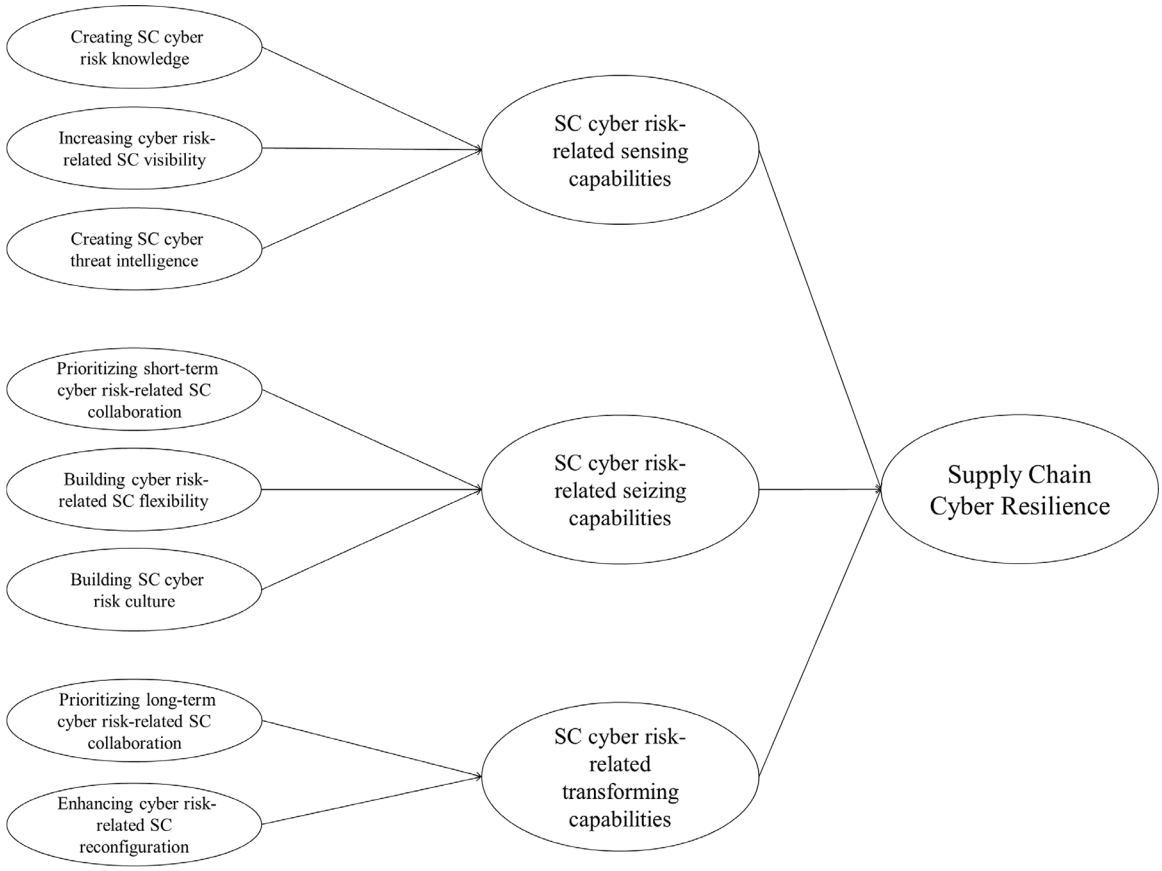
Based on this discussion, we developed a conceptual model (see Figure 2) demonstrating the relationship between DC and SCCR. There are several conceptual models on SCRES in general (Christopher and Peck, 2004; Pettit *et al.*, 2010; Chowdhury and Quaddus, 2016), but to the extent of our knowledge, our conceptualization of the relationship between DC and SCCR provides a new direction for research and scholarship on a better understanding of improving SCCR.

Conclusion

Using DC, this study indicates that managing cyber risks in SCs is a dynamic and complex process that requires different and new SCRES capabilities. SCs need capabilities to shape and realign the SC to address cyber risks. This research shows how SCs can sense and seize cyber threats and risks for building SCCR and demonstrates that it is necessary to identify and develop relevant SC DCs through the deliberate efforts of managers who reconfigure and orchestrate activities for building SCCR. While previous research on SCRES using DC has primarily addressed SCRES in general, this research demonstrates the use of DC in SCRES specific to cyber risks. This viewpoint has provided a solid theoretical framework for examining SCRES. Concerning sensing, seizing and transforming, SCs have a range of actions that can be implemented to build SCCR. The developed propositions add to the extant theory of SCRES to underline how to build SCCR:

- *Sensing*. This research indicates that SCs need three sensing microfoundations – creating SC cyber risk knowledge, increasing cyber risk-related SC visibility and creating SC

Figure 2 SCCR model



Source: Authors own work

cyber threat intelligence – which help to be more alert to cyber risks.

- *Seizing*. SCs need to develop microfoundations – prioritizing short-term cyber risk-related SC collaboration, building cyber risk-related SC flexibility and building SC cyber risk culture – as seizing activities to address sensed cyber threats.
- *Transforming*. In addition to sensing and seizing activities, SCs need transforming capabilities – prioritizing long-term cyber risk-related SC collaboration and enhancing cyber risk-related SC reconfiguration – to help rearrange SC processes.

Implications

Theoretical implications

This research enriches the academic discourse on SCRES by incorporating DC theory, thereby producing notable theoretical advancements. First, by contextualizing DC theory within the framework of SCRES, we provide nuanced interpretations of conventional DCs – sensing, seizing and transforming. Specifically, we adapt these interpretations to the challenges posed by cyber risk in the SC and shed light on their nuanced role in this particular context. Second, the study goes beyond the traditional understanding of DC by unveiling innovative capabilities specifically designed for cyber risk management. These capabilities address the subtleties and complexities unique to cyber threats and represent a significant theoretical extension of the general DC framework. Third, the temporal dimension of our study is emphasized by examining SC collaboration. We emphasize its role as a long-term mechanism that plays a central role across the SC. Rather than viewing SC collaboration merely as a static capability, we present it as an evolving and dynamic process within SCRES. This highlights the importance of time and progress in DC theory and also shows how SC collaboration evolves and adapts over time in response to the ever-changing landscape of cyber threats. Fourth, this research introduces a temporal view of SCRES by detailing the consecutive processes associated with sensing, seizing and transforming capabilities, suggesting resilience as a dynamic property of SCs that evolves, matures and strengthens over time in response to cyber threats. Finally, the study underscores the importance of integrating cyber security expertise in building SCCR, marking a pivotal advancement in both SCRES and DC theory by recognizing the necessity of cross-disciplinary expertise. Collectively, these theoretical implications provide a refined understanding of SCRES through the lens of DC theory while opening avenues for future research.

In addition, this study contributes to discussions about SCRES in general and specifically emphasizing the rising

prevalence of cyber risks. First, we revealed that cyber risks, differing from traditional SC threats, demand agile and different responses by leveraging and sharpening sensing and seizing capabilities. Sensing involves activities to identify and assess the relevant SC cyber risks and complement externally available cyber risk-related information. This aligns and contextualizes the sensing approach in Teece's (2007) conceptual model. Second, the seizing capabilities to address cyber risks in SCs involves short-term SC collaboration and flexibility supported by a cyber risk culture. This definition complements Teece's (2007) concept of seizing and positions it in the context of SCCR. Third, transforming capabilities support long-term changes for addressing sensed and seized SC cyber risks. After addressing cyber risks in the short-term, favorable circumstances that stimulate long-term changes typically vanish once the SC risk is addressed. To stimulate transformation in the DC framework, it is proposed that SCs develop the capacity to maintain long-term changes using SC collaboration and reconfiguration.

DC theory is often criticized for its ambiguity (Ambrosini and Bowman, 2009) and lack of empirical practices (Wang and Ahmed, 2007), which is countered by Sunder *et al.* (2019). However, this empirical research demonstrates overcoming these limitations and increasing DC's explanatory capacity for SCCR. This approach also encourages further theoretical elaboration in SCRES. Furthermore, this study demonstrates that the DC framework suits deploying SCRES and addressing specific SC risks. Finally, combined with SCRES to particular SC risks, the DC framework can also be applied to other SC contexts.

Managerial implications

The results of this research have practical insights for managers both within the case studies and across other SCs. The DCs detailed in this study serve as pivotal elements for establishing SCCR, providing managers with targeted focal points to confront cyber risks. By using the DC framework, practitioners can effectively identify, prioritize and sequence practices, leveraging the interdependencies of the microfoundations. Importantly, this study underscores the need for the co-evolution of resources and capabilities amongst SC partners to foster SCCR, thus, emphasizing the role of inter-organizational collaboration.

Practically, the study underscores the unique characteristics of managing cyber risks, distinguishing it from conventional SC risks. In the face of cyber threats, reliance on IT security expertise becomes crucial, necessitating internal resources or external collaboration. To reduce the reliance on IT security, managers could consider establishing dedicated cyber threat teams to monitor emerging risks and work closely with all SC partners. Simultaneously, it highlights the significance of ongoing education and training for all managerial personnel to enhance comprehension and responsiveness to SC cyber risks. This could translate into quarterly cyber training that is updated based on the latest threats and vulnerabilities, ensuring that executives stay ahead of the curve in their defense strategies. Ultimately, these findings confirm that SC cyber risks require a mix of general SCRES capabilities and specialized competencies to address cyber threats. Consequently, SCM should be willing to explore innovative paths and restructure processes for building SCCR (see Oke and Nair, 2023).

In addition, the unique nature of cybersecurity implies that traditional collaboration and integration strategies may need to be adapted or expanded. For instance, information sharing between SC partners becomes even more critical due to the potential for cyber threats to impact multiple areas simultaneously. Enhanced trust and transparency, along with specific agreements on cyber security standards, could also become important factors in successful collaborations. For example, Woelfl *et al.* (2023) report on a supplier who, during negotiations, promised machinery delivery but concealed a cyber attack affecting their construction plans. Such behavior can permanently damage the collaboration between suppliers and buyers. Similarly, technological integration might require additional attention to secure connectivity, using solutions such as advanced encryption and secure access controls. Thus, in the cybersecurity context, collaboration and integration, which are central to SCRES, take on new dimensions and requirements for building SCCR. Based on this, managers can use proven cybersecurity solutions for encryption and access control features to ensure that their SC is protected from cyber threats.

Limitations and future research

In addition to its implications, this study has limitations that provide opportunities for future research. First, SC cyber risks offer an exciting research avenue due to their characteristics and the potential for a massive and distinct effect on SCs compared to the conventional risks discussed in the literature. Second, it would be interesting to study further SCs that experienced a cyber incident impacting SC assets' availability, confidentiality and integrity, such as the SolarWinds cyber attack in 2021.

The rising reliance on digital SC assets and the dynamic environment certainly creates new opportunities for cybercriminals. Therefore, it is unclear what the future might hold, especially regarding the long-term impacts. In addition, the temporal characteristics of the dynamic environment surrounding cyber risks allow for longitudinal analysis of cyber risks in SCs. Therefore, scholars are invited to study trends related to cyber risks in SCs. This will help examine novel DCs so that SCRES practices to address cyber risks can inspire SC transformation. Finally, this study discusses the SCRES of European industrial SCs in the face of cyber risks. Although the proposed taxonomy has value for the SCRES discourse, future research is needed to elaborate on the performance of an SC with resilience to cyber risks.

References

Al Naimi, M., Faisal, M.N., Sobh, R. and Bin Sabir, L. (2021), "A systematic mapping review exploring 10 years of research on supply chain resilience and reconfiguration", *International Journal of Logistics: Research and Applications*, Vol. 25 No. 8, pp. 1-28.

Ali, I. and Gölgeci, I. (2019), "Where is supply chain resilience research heading? A systematic and co-occurrence analysis", *International Journal of Physical Distribution & Logistics Management*, Vol. 49 No. 8, pp. 793-815.

Ali, I., Gölgeci, I. and Arslan, A. (2023), "Achieving resilience through knowledge management practices and risk management

culture in Agri-food supply chains", *Supply Chain Management: An International Journal*, Vol. 28 No. 2, pp. 284-299.

Ali, A., Mahfouz, A. and Arisha, A. (2017), "Analysing supply chain resilience: integrating the constructs in a concept mapping framework via a systematic literature review", *Supply Chain Management: An International Journal*, Vol. 22 No. 1, pp. 16-39.

Allianz (2023), "Allianz risk barometer", available at: www.allianz.com/content/dam/onemarketing/azcom/Allianz_com/press/document/Allianz-Risk-Barometer-2023.pdf (accessed 5 April 2024).

Alvarenga, M.Z., Oliveira, M.P.V.D. and Oliveira, T. (2023), "The impact of using digital technologies on supply chain resilience and robustness: the role of memory under the covid-19 outbreak", *Supply Chain Management: An International Journal*, Vol. 28 No. 5, pp. 825-842.

Ambrosini, V. and Bowman, C. (2009), "What are dynamic capabilities and are they a useful construct in strategic management?", *International Journal of Management Reviews*, Vol. 11 No. 1, pp. 29-49.

Ambulkar, S., Blackhurst, J. and Grawe, S. (2015), "Firm's resilience to supply chain disruptions: scale development and empirical examination", *Journal of Operations Management*, Vol. 33-34 No. 1, pp. 111-122.

Aslam, H., Blome, C., Roscoe, S. and Azhar, T.M. (2018), "Dynamic supply chain capabilities", *International Journal of Operations and Production Management*, Vol. 38 No. 12, pp. 2266-2285.

Aslam, H., Khan, A.Q., Rashid, K. and Rehman, S. (2020), "Achieving supply chain resilience: the role of supply chain ambidexterity and supply chain agility", *Journal of Manufacturing Technology Management*, Vol. 31 No. 6, pp. 1185-1204.

Bahrami, M. and Shokouhyar, S. (2022), "The role of big data analytics capabilities in bolstering supply chain resilience and firm performance: a dynamic capability view", *Information Technology & People*, Vol. 35 No. 5, pp. 1621-1651.

Bak, O., Shaw, S., Colicchia, C. and Kumar, V. (2020), "A systematic literature review of supply chain resilience in small–medium enterprises (SMEs): a call for further research", *IEEE Transactions on Engineering Management*, Vol. 70 No. 1, pp. 328-341.

Barney, J. (1991), "Firm resources and sustained competitive advantage", *Journal of Management*, Vol. 17 No. 1, pp. 99-120.

Bartol, N. (2014), "Cyber supply chain security practices DNA – filling in the puzzle using a diverse set of disciplines", *Technovation*, Vol. 34 No. 7, pp. 354-361.

Blackhurst, J., Craighead, C.W., Elkins, D. and Handfield, R. B. (2005), "An empirically derived agenda of critical research issues for managing supply-chain disruptions", *International Journal of Production Research*, Vol. 43 No. 19, pp. 4067-4081.

Blome, C., Schoenherr, T. and Rexhausen, D. (2013), "Antecedents and enablers of supply chain agility and its effect on performance: a dynamic capabilities perspective", *International Journal of Production Research*, Vol. 51 No. 4, pp. 1295-1318.

Bravo-Lillo, C., Cranor, L.F., Downs, J. and Komanduri, S. (2011), "Bridging the gap in computer security warnings: a mental model approach", *IEEE Security & Privacy Magazine*, Vol. 9 No. 2, pp. 18-26.

Chowdhury, M.M.H. and Quaddus, M. (2016), "Supply chain readiness, response and recovery for resilience", *Supply Chain Management: An International Journal*, Vol. 21 No. 6, pp. 709-731.

Christopher, M. and Peck, H. (2004), "Building the resilient supply chain", *The International Journal of Logistics Management*, Vol. 15 No. 2, pp. 1-14.

Chunsheng, L., Wong, C.W., Yang, C.-C., Shang, K.-C. and Lirn, T.-C. (2020), "Value of supply chain resilience: roles of culture, flexibility, and integration", *International Journal of Physical Distribution & Logistics Management*, Vol. 50 No. 1, pp. 80-100.

Colicchia, C., Creazza, A. and Menachof, D.A. (2019), "Managing cyber and information risks in supply chains: insights from an exploratory analysis", *Supply Chain Management: An International Journal*, Vol. 24 No. 2, pp. 215-240.

Creazza, A., Colicchia, C., Spiezia, S. and Dallari, F. (2022), "Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era", *Supply Chain Management: An International Journal*, Vol. 27 No. 1, pp. 30-53.

Datta, P.P., Christopher, M. and Allen, P. (2007), "Agent-based modelling of complex production/distribution systems to improve resilience", *International Journal of Logistics Research and Applications*, Vol. 10 No. 3, pp. 187-203.

Drnevich, P.L. and Kriauciunas, A.P. (2011), "Clarifying the conditions and limits of the contributions of ordinary and dynamic capabilities to relative firm performance", *Strategic Management Journal*, Vol. 32 No. 3, pp. 254-279.

Dubois, A. and Gadde, L.-E. (2002), "Systematic combining: an abductive approach to case research", *Journal of Business Research*, Vol. 55 No. 7, pp. 553-560.

Durach, C.F., Wiengarten, F. and Choi, T.Y. (2020), "Supplier–supplier coopetition and supply chain disruption: first-tier supplier resilience in the tetradic context", *International Journal of Operations & Production Management*, Vol. 40 Nos 7/8, pp. 1041-1065.

Eisenhardt, K.M. (1989), "Building theories from case study research", *The Academy of Management Review*, Vol. 14 No. 4, p. 532.

Eisenhardt, K.M. (2021), "What is the Eisenhardt method, really?", *Strategic Organization*, Vol. 19 No. 1, pp. 147-160.

Eisenhardt, K.M. and Graebner, M.E. (2007), "Theory building from cases: opportunities and challenges", *Academy of Management Journal*, Vol. 50 No. 1, pp. 25-32.

Endres, H. and van Bruggen, G.H. (2021), "Two sides of the sensing capability", *Academy of Management Proceedings*, Vol. 2021 No. 1, p. 14819.

ENISA (2022), "ENISA threat landscape 2022", available at: www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (accessed 5 December 2022).

Fiksel, J., Croxton, K.L. and Pettit, T.J. (2015), "From risk to resilience: learning to deal with disruption", *MIT Sloan Management Review*, Vol. 56 No. 2, pp. 78-86.

Fisher, G. and Aguinis, H. (2017), "Using theory elaboration to make theoretical advancements", *Organizational Research Methods*, Vol. 20 No. 3, pp. 438-464.

Flyvbjerg, B. (2006), "Five misunderstandings about case-study research", *Qualitative Inquiry*, Vol. 12 No. 2, pp. 219-245.

Gaudenzi, B., Pellegrino, R. and Confente, I. (2023), "Achieving supply chain resilience in an era of disruptions: a configuration approach of capacities and strategies", *Supply Chain Management: An International Journal*, Vol. 28 No. 7, pp. 438-464.

Ghadge, A., Weiß, M., Caldwell, N.D. and Wilding, R. (2019), "Managing cyber risk in supply chains: a review and research agenda", *Supply Chain Management: An International Journal*, Vol. 25 No. 2, pp. 223-240.

Gioia, D.A., Corley, K.G. and Hamilton, A.L. (2013), "Seeking qualitative rigor in inductive research", *Organizational Research Methods*, Vol. 16 No. 1, pp. 15-31.

Gligor, D., Gligor, N., Holcomb, M. and Bozkurt, S. (2019), "Distinguishing between the concepts of supply chain agility and resilience", *The International Journal of Logistics Management*, Vol. 30 No. 2, pp. 467-487.

Han, Y., Chong, W.K. and Li, D. (2020), "A systematic literature review of the capabilities and performance metrics of supply chain resilience", *International Journal of Production Research*, Vol. 58 No. 15, pp. 4541-4566.

Harland, C.M., Caldwell, N.D., Powell, P. and Zheng, J. (2007), "Barriers to supply chain information integration: SMEs adrift of eLands", *Journal of Operations Management*, Vol. 25 No. 6, pp. 1234-1254.

Helfat, C.E. and Peteraf, M.A. (2009), "Understanding dynamic capabilities: progress along a developmental path", *Strategic Organization*, Vol. 7 No. 1, pp. 91-102.

Hendriksen, C. (2023), "AI for supply chain management: disruptive innovation or innovative disruption?", *Journal of Supply Chain Management*, Vol. 59 No. 3, pp. 65-76.

Hirschman, E.C. (1986), "Humanistic inquiry in marketing research: philosophy, method, and criteria", *Journal of Marketing Research*, Vol. 23 No. 3, p. 237.

Holgado, M. and Niess, A. (2023), "Resilience in global supply chains: analysis of responses, recovery actions and strategic changes triggered by major disruptions", *Supply Chain Management: An International Journal*, Vol. 28 No. 6.

Holling, C.S. (1973), "Resilience and stability of ecological systems", *Annual Review of Ecology and Systematics*, Vol. 4 No. 1, pp. 1-23.

Holling, C.S. (1996), "Engineering resilience versus ecological resilience", in Schulze, P. (Ed.), *Engineering within Ecological Constraints*, National Academy Press, Washington, DC, pp, pp. 31–43.

Ivanov, D. and Das, A. (2020), "Coronavirus (COVID-19/SARS-CoV-2) and supply chain resilience: a research note", *International Journal of Integrated Supply Management*, Vol. 13 No. 1, pp. 90-102.

Ivanov, D. and Dolgui, A. (2021), "Stress testing supply chains and creating viable ecosystems", *Operations Management Research*, Vol. 15 No. 1-2, pp. 1-12.

Jones, K.S., Lodinger, N.R., Widlus, B.P., Namin, A.S. and Hewett, R. (2021), "Do warning message design recommendations address why non-experts do not protect themselves from cybersecurity threats? A review", *International Journal of Human–Computer Interaction*, Vol. 37 No. 18, pp. 1709-1719.

Jüttner, U. and Maklan, S. (2011), "Supply chain resilience in the global financial crisis: an empirical study", *Supply Chain Management: An International Journal*, Vol. 16 No. 4, pp. 246-259.

Ketokivi, M. and Choi, T. (2014), "Renaissance of case research as a scientific method", *Journal of Operations Management*, Vol. 32 No. 5, pp. 232-240.

Kochan, C.G. and Nowicki, D.R. (2018), "Supply chain resilience: a systematic literature review and typological framework", *International Journal of Physical Distribution & Logistics Management*, Vol. 48 No. 8, pp. 842-865.

Kulp, S.C., Lee, H.L. and Ofek, E. (2004), "Manufacturer benefits from information integration with retail customers", *Management Science*, Vol. 50 No. 4, pp. 431-444.

Lincoln, Y.S. and Guba, E.G. (1985), "Establishing trustworthiness", *Naturalistic Inquiry*, Vol. 331 No. 289, pp. 289-327.

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.

Melnyk, S.A., Davis, W.E., Spekman, R.E. and Sandor, J. (2010), "Outcome-driven supply chains", *MIT Sloan Management Review*, Vol. 51 No. 2, pp. 32-38.

Melnyk, S.A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J.F. and Friday, D. (2022), "New challenges in supply chain management: cybersecurity across the supply chain", *International Journal of Production Research*, Vol. 60 No. 1, pp. 162-183.

Miles, M.B., Huberman, A.M. and Saldaña, J. (2020), *Qualitative Data Analysis: A Methods Sourcebook*, 4th edition Sage, Los Angeles.

Mollenkopf, D.A., Frankel, R. and Russo, I. (2011), "Creating value through returns management: exploring the marketing-operations interface", *Journal of Operations Management*, Vol. 29 No. 5, pp. 391-403.

Mubarik, M.S., Naghavi, N., Mubarik, M., Kusi-Sarpong, S., Khan, S.A., Zaman, S.I. and Kazmi, S.H.A. (2021), "Resilience and cleaner production in industry 4.0: role of supply chain mapping and visibility", *Journal of Cleaner Production*, Vol. 292, pp. 1-12.

Müller, M. and Gaudig, S. (2011), "An empirical investigation of antecedents to information exchange in supply chains", *International Journal of Production Research*, Vol. 49 No. 6, pp. 1531-1555.

Nikookar, E., Stevenson, M. and Varsei, M. (2024), "Building an antifragile supply chain: a capability blueprint for resilience and post-disruption growth", *Journal of Supply Chain Management*, Vol. 60 No. 1, pp. 13-31.

Oke, A. and Nair, A. (2023), "From chaos to creation: the mutual causality between supply chain disruption and innovation in low-income markets", *Journal of Supply Chain Management*, Vol. 59 No. 3, pp. 20-41.

Pandey, S., Singh, R.K., Gunasekaran, A. and Kaushik, A. (2020), "Cyber security risks in globalized supply chains: conceptual framework", *Journal of Global Operations and Strategic Sourcing*, Vol. 13 No. 1, pp. 103-128.

Pérez-Nordtvedt, L., Khavul, S., Harrison, D.A. and McGee, J.E. (2014), "Adaptation to temporal shocks: influences of

strategic interpretation and spatial distance", *Journal of Management Studies*, Vol. 51 No. 6, pp. 869-897.

Pettit, T.J., Croxton, K.L. and Fiksel, J. (2013), "Ensuring supply chain resilience: development and implementation of an assessment tool", *Journal of Business Logistics*, Vol. 34 No. 1, pp. 46-76.

Pettit, T.J., Croxton, K.L. and Fiksel, J. (2019), "The evolution of resilience in supply chain management: a retrospective on ensuring supply chain resilience", *Journal of Business Logistics*, Vol. 40 No. 1, p. 347.

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.

Ponomarov, S.Y. (2012), "Antecedents and consequences of supply chain resilience: a dynamic capabilities perspective", Dissertation, University of Tennessee, Knoxville, TN.

Queiroz, M.M., Fosso Wamba, S. and Branski, R.M. (2021), "Supply chain resilience during the COVID-19: empirical evidence from an emerging economy", *Benchmarking: An International Journal*, Vol. 29 No. 6, pp. 1999-2018.

Radanliev, P., Roure, D., de, Page, K., Nurse, J., R., C., Mantilla Montalvo, R., Santos, O., Maddox, L. and Burnap, P. (2020), "Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains", *Cybersecurity*, Vol. 3 No. 1, pp. 1-21.

Renaud, K., Flowerday, S., Warkentin, M., Cockshott, P. and Orgeron, C. (2018), "Is the responsibilization of the cyber security risk reasonable and judicious?", *Computers & Security*, Vol. 78, pp. 198-211.

Rice, J.B. and Caniato, F. (2003), "Building a secure and resilient supply network", *Supply Chain Management Review*, Vol. 7 No. 5, pp. 22-30.

Richey, R.G., Roath, A.S., Adams, F.G. and Wieland, A. (2022), "A responsiveness view of logistics and supply chain management", *Journal of Business Logistics*, Vol. 43 No. 1, pp. 62-91.

Roh, J., Tokar, T., Swink, M. and Williams, B. (2022), "Supply chain resilience to low-/high-impact disruptions: the influence of absorptive capacity", *The International Journal of Logistics Management*, Vol. 33 No. 1, pp. 214-238.

Russo, I., Pellathy, D. and Omar, A. (2021), "Managing outsourced reverse supply chain operations: middle-range theory development", *Journal of Supply Chain Management*, Vol. 57 No. 4, pp. 63-85.

Sáenz, M.J. and Revilla, E. (2014), "Creating more resilient supply chains", *MIT Sloan Management Review*, Vol. 55 No. 4, pp. 22-24.

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.

Scholten, K., Sharkey Scott, P. and Fynes, B. (2014), "Mitigation processes – antecedents for building supply chain resilience", *Supply Chain Management: An International Journal*, Vol. 19 No. 2, pp. 211-228.

Strupczewski, G. (2021), "Defining cyber risk", *Safety Science*, Vol. 135, pp. 1-10.

Scholten, K., Sharkey Scott, P. and Fynes, B. (2019), "Building routines for non-routine events: supply chain resilience learning mechanisms and their antecedents", *Supply Chain Management: An International Journal*, Vol. 24 No. 3, pp. 430-442.

Sunder, V.M., Ganesh, L.S. and Marathe, R.R. (2019), "Dynamic capabilities", *European Business Review*, Vol. 31 No. 1, pp. 25-63.

Taddeo, M., McCutcheon, T. and Floridi, L. (2019), "Trusting artificial intelligence in cybersecurity is a double-edged sword", *Nature Machine Intelligence*, Vol. 1 No. 12, pp. 557-560.

Teece, D.J. (2007), "Explicating dynamic capabilities: the nature and microfoundations of (sustainable) enterprise performance", *Strategic Management Journal*, Vol. 28 No. 13, pp. 1319-1350.

Teece, D., Peteraf, M. and Leih, S. (2016), "Dynamic capabilities and organizational agility: risk, uncertainty, and strategy in the innovation economy", *California Management Review*, Vol. 58 No. 4, pp. 13-35.

Teece, D.J., Pisano, G. and Shuen, A. (1997), "Dynamic capabilities and strategic management", *Strategic Management Journal*, Vol. 18 No. 7, pp. 509-533.

Tran, T.T.H., Childerhouse, P. and Deakins, E. (2016), "Supply chain information sharing. Challenges and risk mitigation strategies", *Journal of Manufacturing Technology Management*, Vol. 27 No. 8, pp. 1102-1126.

Tukamuhabwa, B.R., Stevenson, M., Busby, J. and Zorzini, M. (2015), "Supply chain resilience: definition, review and theoretical foundations for further study", *International Journal of Production Research*, Vol. 53 No. 18, pp. 5592-5623.

Umar, M., Wilson, M. and Heyl, J. (2021), "The structure of knowledge management in inter-organisational exchanges for resilient supply chains", *Journal of Knowledge Management*, Vol. 25 No. 4, pp. 826-846.

Vanpoucke, E., Boyer, K.K. and Vereecke, A. (2009), "Supply chain information flow strategies: an empirical taxonomy", *International Journal of Operations & Production Management*, Vol. 29 No. 12, pp. 1213-1241.

von Solms, R. and van Niekerk, J. (2013), "From information security to cyber security", *Computers & Security*, Vol. 38, pp. 97-102.

Voss, C., Johnson, M. and Godsell, J. (2016), "Case research", in Karlsson, C. (Ed.), *Research Methods for Operations Management*, 2nd ed., Routledge, New York, NY, pp. 165-197.

Walker, B.H. (2020), "Resilience: what it is and is not", *Ecology and Society*, Vol. 25 No. 2, pp. 1-3.

Wang, C.L. and Ahmed, P.K. (2007), "Dynamic capabilities: a review and research agenda", *International Journal of Management Reviews*, Vol. 9 No. 1, pp. 31-51.

Wernerfelt, B. (1984), "A Resource-Based view of the firm", *Strategic Management Journal*, Vol. 5 No. 2, pp. 171-180.

Wieland, A. (2021), "Dancing the supply chain: toward transformative supply chain management", *Journal of Supply Chain Management*, Vol. 57 No. 1, pp. 58-73.

Wieland, A. and Durach, C.F. (2021), "Two perspectives on supply chain resilience", *Journal of Business Logistics*, Vol. 42 No. 3, pp. 315-322.

Wieland, A., Stevenson, M., Melnyk, S.A., Davoudi, S. and Schultz, L. (2023), "Thinking differently about supply chain resilience: what we can learn from social-ecological systems

thinking", *International Journal of Operations & Production Management*, Vol. 43 No. 1, pp. 1-21.
Winter, S.G. (2003), "Understanding dynamic capabilities", *Strategic Management Journal*, Vol. 24 No. 10, pp. 991-995.
Woelfl, K., Kaufmann, L. and Carter, C.R. (2023), "In the eye of the beholder: a configurational exploration of perceived deceptive supplier behavior in negotiations", *Journal of Supply Chain Management*, Vol. 59 No. 2, pp. 33-61.
Yaroson, E.V., Breen, L., Hou, J. and Sowter, J. (2021), "Advancing the understanding of pharmaceutical supply chain resilience using complex adaptive system (CAS) theory", *Supply Chain Management: An International Journal*, Vol. 26 No. 3, pp. 323-340.
Yin, R.K. (2014), *Case Study Research: Design and Methods*, Fifth edition Sage, Los Angeles.
Zouari, D., Ruel, S. and Viale, L. (2021), "Does digitalising the supply chain contribute to its resilience?", *International Journal of Physical Distribution & Logistics Management*, Vol. 51 No. 2, pp. 149-180.

Further reading

Kähkönen, A.-K., Evangelista, P., Hallikas, J., Immonen, M. and Lintukangas, K. (2021), "COVID-19 as a trigger for dynamic capability development and supply chain resilience improvement", *International Journal of Production Research*, Vol. 61 No. 8, pp. 1-20.
Teece, D.J. (2014), "The foundations of enterprise performance: dynamic and ordinary capabilities in an (economic) theory of firms", *Academy of Management Perspectives*, Vol. 28 No. 4, pp. 328-352.

Appendix 1. Abbreviated interview protocol

I grouped the following questions according to SCRES, cyber risks in SCs and the three DCs:

2 SCRES

- Capabilities to adapt, prepare, respond, recover, grow
- Experience with SC disruptions, good and bad examples
- Current methods and approaches to deal with risks

3 Cyber risks

- Role of cyber risks in SCs
- Current methods and approaches to deal with SC cyber risks

4 Sensing capabilities

- How do or would you scan and monitor cyber risks in your SC?
- How do or would you identify SC cyber risks?
- How do or would you share the information, and with whom?
- What is the relevant SC?

5 Seizing capabilities

- How do or would you address the sensed SC cyber risks?
- What SC structures and processes support you in addressing the sensed SC cyber risks?
- What are the short-term aspects to consider in sensing?

6 Transforming capabilities

- What do or would you change long-term to address the sensed and seized SC cyber risks?
- With which resources and competencies do you align or realign to address the cyber risks in your SC?

Appendix 2

Table A1 Trustworthiness of the study and findings

Criterion	Tactic from literature	Implementation in this research
Construct validity	• Use multiple sources of evidence	• Multiple interviews in each stage of the SC, multiple companies and site visits; workshops with all participants; additional documents reviewed
	• Establish a chain of evidence	• Key informants reviewed the case write-up and the report before submission. Feedback was sought from all participants
	• Key informant review draft of the case study report	• Transcripts of the interview were provided to participants for feedback and evaluation
Internal validity	• Pattern matching	• Patterns regarding SCRES were investigated
	• Explanation building	
	• Rival explanations	
External validity	• Use replication logic in multiple case studies	• Four cases were used for replicability of constructs and proposed theoretical relationships
Reliability	• Use case study protocol	• A case study protocol was defined and implemented
	• Develop case study database	• A case study database was created and used
Credibility	• Data from all participants represent the concepts	• Evidence from all participants is used to support the concepts
	• Adopt well-established research methods	• The research followed suggested procedures (Eisenhardt, 1989; Dubois and Gadde, 2002; Eisenhardt and Graebner, 2007)
	• Triangulate interviews with supporting data	• Additional documents were used for validating interview data
	• Use iterative questioning	• Participants were contacted multiple times for follow-up and clarification
Dependability	• Participants reflect on multiple experiences	• A cross-case analysis was used to record responses for each participant
		• Interviews were open-ended, discovery-oriented and lasted from 25 to 165 min
Conformability	• Nonthreatening and anonymous interviews	• Open-ended questions allowed participants to reflect on experiences
Integrity	• Maintain professional conduct	• Interviews were conducted professionally and in a nonthreatening manner; all interviews were recorded and transcribed afterward
	• Use a diverse set of participants	• Interviews included numerous participants who were highly knowledgeable in the underlying research topic

Source: Author's own work

Appendix 3. Brief individual case overview

Each case is briefly summarized in the following paragraphs. This includes a concise description of the SC and an overview of the role of cyber risks, SCM and SCRES.

SteSC

SteSC's (representing an SC with triadic relation) focal company, SteCo, is a multinational technology group in the raw material sector. All participating SC partners' headquarters are located in Central Europe. Four customers and Supplier 1 are also multinationals. Three of the customers are manufacturers of industrial supplies. The fourth is a mechanical engineering company. While Supplier 1 supplies industrial products to SteCo, the other two suppliers are small-sized enterprises that offer media technology and digital services. SteCo has a longstanding relationship with all partners, and most of the selected partners are crucial for SteCo. All customers, SteCo and Supplier 1 have an IT security department in-house. Parts of the focal company and Customer 1 are ISO 27001 certified.

Suppliers 2 and 3 have outsourced their IT security departments, Supplier 2 additionally its IT department. All companies of SteSC face heightened cyber security concerns in their SC and industries. Although none of SteCo's participating customers are directly from the automotive industry, two are downstream of automotive SCs and recognize heightened cyber security requirements based on TISAX. All companies have in common that their main cyber risk concerns are related to IT SCs, with little focus on OT and almost no focus on other SCs, such as raw materials. While SC disruptions play a daily role in this SC, this SC has also been affected by cyber attacks in recent years. Supplier 1 experienced a cyber attack during this project, which allowed this research to examine the impact on the SC in detail. In addition, SteCo and two of its customers (SteSC2 and

SteSC4) were also affected by several cyber attacks in their SC that affected other companies not included in this study. However, this enabled the study to elaborate on these SC impacts and experiences.

CriSC

CriCo, the focal company of CriSC (representing an SC with tetradic relation), is a supplier to the critical infrastructure and manufacturing industries with many locations in Central Europe and has been fully ISO 27001 certified for years. The company supplies industrial applications and smart products to its customers, who require different standards and norms for their SC, depending on the industry. Therefore, IT security plays an essential role in the various SC processes at CriSC, as do IT security certifications, most notably ISO 27001. While the IT departments of the two customers are also certified to the same standard, the participating suppliers and subsuppliers are not. Compared to the other cases in this study, CriSC is the SC with the highest level of maturity in dealing with cyber risks along the SC. It is interesting to note that the requirements for SC partners decrease further downstream in the SC.

CriCo's direct supplier is a medium-sized enterprise that provides electronics manufacturing services to its customers. It has its own IT department, but IT security is outsourced; the same applies to the first subsupplier, a small-sized enterprise. Supplier CriSC1 experienced a ransomware attack two years ago, which affected the availability of goods and services for CriSC. In addition, customers CriSC1 and CrisSC2, as large national corporations, have experienced many cyber attacks in their SC, but again, only availability was affected, not the integrity or confidentiality of SC assets. CriCo recognized SolarWinds' cyber attack in 2021 as a cyber risk that indirectly impacted its SC assets.

InsSC

InsCo, an industrial automation manufacturer, is the focal company of InsSC (representing an SC with triadic relation) and is a multinational group headquartered in Central Europe. InsCo's products are used in production environments worldwide to increase the automation and digitalization of OT processes. All three customers involved are manufacturers or producers of industrial products that use InsCo's products as components for their end products. Three suppliers deliver industrial products to InsCo, which assembles them with other parts to create end products. The fourth supplier is a logistics service provider that operates worldwide. InsCo maintains a long-term relationship with all SC partners involved.

All companies involved in InsSC have their own IT security department that focuses mainly on their own IT SC, without considering the SC as a whole, including OT and raw material supplies. In addition, the IT departments of InsCo and Supplier 4 are ISO 27001 certified. Cyber risk-related activities between SC members play a minor role. Most SC activities focus on product availability, price and quality. InsCo was directly affected by a cyber attack on Supplier 1 in 2019.

ComSC

The fourth SC, ComSC (representing an SC with triadic relation), contains companies in the construction industry, with ComCo as the focal company. ComCo is a construction machinery manufacturer with headquarters in Central Europe, and it has its own IT security department, like all other companies reflecting this SC. ComCo's customers all operate in the construction industry and are multinational organizations. ComCo's products supplied to its customers are at an early stage of digitalization compared to other industries. The suppliers involved are logistics service providers and manufacturers of industrial products. Both are multinational, globally operating groups with headquarters in Central Europe.

Although all companies have an internal IT security department, there are almost no SC activities related to cyber risks. ComCo, for example, only started to build an IT security department a few years ago. This probably also explains the low level of maturity of activities related to cyber risks in the SC. In addition, digitalization has just started to play a significant role in this industry, and awareness about SC cyber threats and risks is still low. ComCo has not yet experienced a direct cyber incident in its SC, but some of the case companies involved have experienced a cyber attack on other SC partners that were not included in this study.

Corresponding author

Michael Herburger can be contacted at: michael.herburger@fh-steyr.at