The International Journal of Logistics Management

Cyber resilience in organisations and supply chains: from perceptions to actions

Barbara Gaudenzi and Benedetta Baldi
Department of Management, University of Verona, Verona, Italy

Received 5 September 2023
Revised 10 January 2024
30 May 2024
30 July 2024
Accepted 8 September 2024

Abstract

Purpose – This empirical study investigates the direct and indirect effects on managers' perceptions of cyber risks, the implementation of cyber resilience strategies and the perceived effectiveness of these strategies for supply chains. Cyber risks pose significant threats to organisations and supply chains. Yet they remain insufficiently addressed and managed.

Design/methodology/approach – Primary data were collected from a sample of Italian organisations using a survey. The structural equation modelling methodology was employed to empirically investigate cyber resilience strategies in supply chains.

Findings – Results indicate that effective cyber resilience is linked to awareness of the negative impacts of cyber risks, particularly supply chain disruptions. This awareness leads to the adoption of various cyber resilience strategies. According to managers' perceptions, several strategies are identified in the study as the most effective in enhancing the cyber resilience supply chains. The findings offer insights for managers regarding the relationship between cyber risk perceptions, supply chain cyber resilience strategies and their effectiveness. These relationships are studied using the theory of perceived risk and the dynamic capabilities theory.

Originality/value – This study advances knowledge for academics and practitioners in the fields of supply chain resilience and supply chain risk management. It contributes to the development of a risk-based thinking model in organisations and supply chains by drawing upon a dual theoretical perspective.

Keywords Cyber resilience, Cyber risk, Supply chain, Business interruption, Reputation

Paper type Research paper

1. Introduction

Organisations and supply chains (SCs) are more vulnerable than ever in today's complex business environment. Accordingly, supply chain resilience (SCRES) has attracted increasing attention from academia, as major disruptions have started threatening SCs with severe consequences (Gaudenzi *et al.*, 2023; Heckmann *et al.*, 2015; Wieland and Wallenburg, 2013).

Several studies have focused on organisations' value creation and competitiveness, investigating how to assess and mitigate the key risks that can impact SC processes (Fan and Stevenson, 2018). However, even though the Supply Chain Risk Management (SCRM) and SCRES literature has grown significantly in recent years, few studies have focused on SCRES for the emergent and under-investigated threat of cyber risks (Ivanov, 2022; Colicchia *et al.*, 2019; Melnyk *et al.*, 2022).

In these times of digital transformation, technology adoption and digitalisation can represent an opportunity to increase supply chain performance and better cope with risks

The initial design of this research is based upon work supported by Fondazione Cariverona, Bando Ricerca e Sviluppo, 2019 (ID 11163 -Cod.SIME 2019.0418).

The International Journal of Logistics Management
Vol. 35 No. 7, 2024
pp. 99-122
Emerald Publishing Limited
0957-4093
DOI 10.1108/IJLM-09-2023-0372

(Ivanov and Dolgui, 2020; Maheshwari *et al.*, 2023). However, digital systems can become significant vulnerabilities for organisations and SCs if effective prevention and protection strategies against cyber threats are not implemented (Ram and Zhang, 2020; Rehman and Ali, 2021).

Ram and Zhang (2020) underlined how "cyber security should not be ignored since technology plays an increasingly significant role in various industries, especially in the SC" (p. 786). Furthermore, several reports have highlighted how cyber risks are growing in severity and frequency, being listed among the top 10 risks for companies and as a primary source of business interruption (Allianz, 2023; Protiviti, 2023; World Economic Forum, 2023). In this context, Eling and Schnell (2016) described cyber risk as "any risk arising from the usage of information technology (IT) that compromises the confidentiality, availability, or integrity of services or data" (p. 483), shedding light on the importance of carefully assessing and managing these threats.

The cybersecurity framework of the National Institute of Standards and Technology (NIST Framework) has stressed the importance of building robust cybersecurity to ensure resilience in organisations and SCs, and scholars have underlined the impact of cyber-physical systems on SCRES (Rehman and Ali, 2021). Besides the "technical dimensions" of cybersecurity, academics take a wider perspective, considering cyber risks as a key threat that organisations must manage from a SCRM perspective (Ivanov, 2022).

However, despite the recognised importance of cyber risks for SCs, this area remains under-investigated. This is primarily due to uncertainty and lack of knowledge about cyber risks, including their likelihood, severity, and the assessment of their impacts (Confente *et al.*, 2019; Ghadge *et al.*, 2019). In this uncertain scenario, where managers lack robust information about cyber risks but must still make proactive decisions, two theoretical lenses can help interpret and address cyber resilience: (1) the theory of perceived risk (TPR) (Jia *et al.*, 1999; Wang *et al.*, 2013), and (2) the dynamic capability theory (DCT) (Teece *et al.*, 2016).

This study aims to investigate the direct and indirect effects on managers' cyber risk perceptions, their adoption of cyber resilience strategies, and the perceived effectiveness of cyber resilience (PECR) among a sample of Italian firms, to establish an enhanced risk-based thinking model. As highlighted by previous studies, the first challenge for decision-makers is achieving cyber risk awareness (Davis, 2015; Eling and Wirfs, 2019) as a precondition for adopting a multi-functional portfolio of strategies to achieve cyber resilience. Beyond traditional reactive approaches to cyber risks, which typically rely on IT tools (Stallings, 2018), decision-makers should proactively evaluate cyber risks and its potential impacts across all key processes. This involves defining the most appropriate mitigation strategies for the organisation and the entire SC, thus contributing to building cyber resilience. Therefore, this study aims to investigate how managers (1) perceive their exposure to cyber risks and the related consequences for the organisation and supply chain; (2) invest in different cyber resilience strategies along the supply chain; and (3) perceive the effectiveness of cyber resilience after adopting the cyber resilience strategies.

2. Theoretical background and hypothesis development

2.1 TPR and DCT

The current research builds upon two theoretical lenses, which allow researchers to interpret the perceived consequences of cyber risks through the TPR and analyse the dynamic investment paths in cyber resilience strategies using the DCT.

TPR, first proposed by Taylor (1974), has been widely used in marketing and SC management studies to shape and interpret consumers' perceptions. TPR suggests that perceived risk can influence consumers' decisions and partially mediate the relationship between perceived quality and perceived value along SCs (Wang *et al.*, 2013).

In our theoretical model, the perceived risk is the cyber threat, and perceptions are related to the specific dimensions of cyber risk consequences (Yang *et al.*, 2020) and the effectiveness of cyber resilience strategies (Kanwal *et al.*, 2022). These perceptions are exposed to subjective evaluations, which in turn influence decision-making processes. The extension of TPR to the supply chain domain was first proposed by Wang *et al.* (2013) and is originally applied here to the concept of cyber resilience. The perceived risks were identified as mainly related to the financial, performance, and social dimensions (Grewal *et al.*, 1994). For example, Jia *et al.* (1999) proposed measures of perceived risk, demonstrating that decision-makers' perception of risk increased with the perceived relevance of expected loss. Thus, applying TPR to cyber risks in the SC context represents a novel area of investigation. Jia *et al.* (1999) established the relationship between perceived risk and the preference for different behaviours (i.e. approaches to mitigate that risk), underlining a "connection between perceived risk and preference" (p. 530). TPR, therefore, offers an important theoretical lens to study cyber resilience, particularly justifying the investigation of varying perceptions about the consequences of cyber risks in the supply chain. TPR grounds the assumptions that in uncertain situations such as emergent and fast-changing cyber risks, most decision-makers' perceptions of cyber risks are influenced by the expected negative consequences along SCs (i.e. in this study, business interruption and/or reputational damage). These perceptions, in turn, influence their decision-making processes.

The second theoretical lens of this study is the DCT (Teece, 2007; Teece *et al.*, 1977), which inspires organisations to integrate, build, and reconfigure their competencies to cope with change. It offers a lens to comprehend and manage the emergent threat of cyber risks with a dynamic perspective.

Regarding cyber risks and cyber risk management, despite the extensive literature on guidelines and frameworks, organisations need to bridge the gap between their investments in cyber risk management and actual cyber resilience. Hence, we build on the substantial literature on dynamic capabilities and their influence on achieving SCRES in complex business environments (Dubey *et al.*, 2023; Fainshmidt *et al.*, 2016) to address multi-faceted risks and disruptions (Queiroz *et al.*, 2022, 2023). In this research, the DCT explores the links between perceived consequences of cyber risks, cyber resilience capabilities and strategies, and the PECR, explaining the different paths firms take to implement cyber resilience (Schilke, 2014). The DCT emphasises the necessary reconfiguration of an organisation's resources and capabilities, moving beyond standard routines and practices outlined in guidelines and frameworks to develop key capabilities to cope with evolving and fast-changing scenarios, such as those posed by cyber threats.

In this study, we considered four cyber resilience strategies that organisations can configure differently. To truly understand the effectiveness and implementation pathways of these strategies, it is crucial to focus on their antecedents. These are inherently represented by their related capabilities, whose configurations in a dynamic view can drive the organisation towards its goal (Fainshmidt *et al.*, 2016, 2019), that is, cyber resilience. Hence, this study's four cyber resilience strategies can be linked to their respective antecedents, according to the capabilities related to the "strategic sense-making capacity", as categorised by Li and Liu (2014).

The link between cyber resilience strategies and related capabilities is developed according to Teece *et al.* (2016), who conceptualised uncertainty, risk, capabilities, and strategies together. These authors underline how strategies and their related capabilities must be developed and implemented together to achieve the goals. Teece *et al.* (2016) stated, "The framework to assist managers in reconceptualising their task, given the absence of market mechanisms for hedging such uncertainty, is dynamic capabilities" (p. 15). Therefore, the DCT explains how cyber resilience strategies and related capabilities can be differently configured and chosen dynamically as a result of a learning process based on increasing awareness about these threats and the selection of reliable cyber resilience strategies.

2.2 SCRM and cyber risks

The SCRM literature addresses the importance of managing key risks that can damage the value creation and competitiveness of organisations and their SCs (Christopher and Peck, 2004; Fan and Stevenson, 2018). Several studies on SCRES have focused on the management of disruptive events that can cause severe business disruptions for organisations and SCs (Gaudenzi *et al.*, 2023; Jüttner and Maklan, 2011; Wieland and Wallenburg, 2013). However, only a few have focused on the emergent but under-investigated threat of cyber risks (Friday *et al.*, 2024; Ivanov, 2022; Colicchia *et al.*, 2019; Melnyk *et al.*, 2022) to build cyber resilience (Perera *et al.*, 2022). Most of these studies have focused on theoretical models and the most adopted frameworks, advocating the need for empirical investigation (Ram and Zhang, 2020; Culot *et al.*, 2021).

2.3 Consequences of cyber risks and cyber resilience strategies

Addressing emergent and fast-changing risks and their associated loss exposure poses a challenge due to limited knowledge and historical experience (Baghersad and Zobel, 2022). This challenge is particularly relevant in the case of cyber risks, where managers must make proactive decisions even in the absence of adequate or robust information. They rely on their perceptions of the potential negative consequences on SCs (Confente *et al.*, 2019; Ghadge *et al.*, 2019; Melnyk *et al.*, 2022).

Some authors have investigated the potential consequences of cyber risks for SCs (Ogbanufe *et al.*, 2021; Yang *et al.*, 2020; Li *et al.*, 2019; Wirtz and Weyerer, 2017), primarily categorising them into two main areas: reputational damage (Burt, 2019; Carnovale and Yeniyurt, 2021) and business interruption along the supply chain (De Gusmão *et al.*, 2018). This underscores the importance of analysing the relationship between perceptions and risk mitigation in the SCs (Arcuri *et al.*, 2020; Diesch *et al.*, 2020). Furthermore, other studies have highlighted the need to coordinate strategies, managerial behaviours, and human resources across different functions and processes to develop effective governance models for cyber resilience in SCs (Bartol, 2014; Creazza *et al.*, 2022).

The adoption of governance strategies and policies under the lens of the DCT has been only partially investigated. Teece *et al.* (2016) underlined the importance of dynamically developing ad-hoc capabilities and approaches to achieve effective and firm-centric implementation of governance and policies to cope with the dynamic legal environment that characterises different industries and organisations. Accordingly, we formulated the following hypotheses to investigate the link between the perception of the two typologies of cyber risk consequence (i.e. potential business interruption awareness PBIA and potential reputation demage awareness PRDA) (Ogbanufe *et al.*, 2021) and the commitment to adopting cyber risk governance strategies and policies (CRGSP) (Kanwal *et al.*, 2022; Ram and Zhang, 2020):

H1. When managers perceive potential business interruption along the supply chain due to cyber risks, there is a commitment to adopting CRGSP for the organisation and the SC.

H2. When managers perceive potential reputational damage due to cyber risks, there is a commitment to adopting CRGSP for the organisation and the SC.

Training programmes for employees in organisations have been recognised as crucial drivers for identifying and managing multifaceted cyber risks (ISO/IEC 27001, 2022; NIST Framework; Tambe *et al.*, 2022; Windelberg, 2016). Cyberattacks can stem from internal personnel or external actors and can have different manifestations (Confente *et al.*, 2019).

From a DC perspective, Easterby-Smith and Prieto (2008) addressed the different configurations of ad-hoc capabilities related to knowledge management and training

programmes, according to different learning perspectives that characterised each organisation. Therefore, training programmes should be customised and run regularly to upskill the organisation's employees to identify, avoid, and respond to all the criticalities of cyber risks (Bulgurcu *et al.*, 2010; Kanwal *et al.*, 2022; Singh *et al.*, 2014). This led to the following hypotheses:

H3. When managers perceive potential business interruption along the supply chain due to cyber risks, there is a commitment to implementing Cyber Security Training (CST) programmes for the employees and partners (SC key actors).

H4. When managers perceive potential reputational damage due to cyber risks, there is a commitment to implementing CST programmes for the employees and partners (key SC actors).

Risk control strategies play a key role in successfully dealing with cyber risks—for instance, investments in IT and operational technology (OT) systems/equipment and software to protect all the SC processes and organisational assets (Kanwal *et al.*, 2022). These tools are typically managed by IT managers in coordination with key decision-makers in different functions, and they require a holistic and shared risk-based view to be effectively implemented and managed (Mazzoccoli and Naldi, 2020; Tambe *et al.*, 2022). These tools focus on guaranteeing continuity to the IT functions and the ERP systems throughout the organisation's processes and along the entire SC.

From a DC perspective, Arena *et al.* (2013) studied how different configurations of risk control strategies and their related dynamic capabilities can lead to building different "dynamic response maps" against risks according to the specific characteristics of the organisation. Hence, we stated the following hypotheses:

H5. When managers perceive potential business interruption along the supply chain due to cyber risks, there is a commitment to adopting cyber risk control (CRC) strategies.

H6. When managers perceive potential reputational damage due to cyber risks, there is a commitment to adopting CRC strategies.

Cyber insurance plays a significant role in managing cyber resilience by contributing to the recovery from risk consequences and offering incentives to invest more in cyber resilience strategies (Meland *et al.*, 2015). Cyber insurance can protect the cash flows of companies experiencing the consequences of cyberattacks (Camillo, 2017; Romanosky *et al.*, 2019). However, several studies have underlined how insurance investments for cyber risks are still scarce and can be differently designed (Ogbanufe *et al.*, 2021), shedding light on the importance of investigating the commitment to invest in these specific tools (Marotta *et al.*, 2017).

From a DC perspective, Stechemesser *et al.* (2015) studied different configurations of risk insurance solutions and programmes according to the specific characteristics of the organisation to achieve insurance protection against risks. Based on that, we proposed the following hypotheses:

H7. When managers perceive potential business interruption along the supply chain due to cyber risks, there is a commitment to investing in cyber risk insurance (CRI).

H8. When managers perceive potential reputational damage due to cyber risk, there is a commitment to investing in CRI.

Adoption of the above-mentioned cyber resilience strategies and the related capabilities allows organisations and their SCs to assess cyber risks and mitigate their negative consequences (Bartol, 2014; Safa *et al.*, 2016).

Measuring the "real" effectiveness and benefits of cyber resilience strategies once negative events occur is not enough. Contrarily, robust cyber resilience is based on a continuous improvement approach, where incremental investments should be linked to the ability to address the effectiveness of the cyber resilience management process in place (Collier *et al.*, 2014, ISO 28000, 2007; ISO/IEC 27001, 2022). Teece *et al.* (2016) and Kosutic and Pigni (2022) addressed the importance of a dynamic approach towards the selection of the most reliable portfolio of cyber resilience strategies through the lens of dynamic capabilities. This underlines the importance of addressing cyber risks as technical problems and developing a specific set of dynamic cyber resilience and cybersecurity capabilities for the SC. Thus, we formulated the following hypotheses:

H9. The adoption of CRGSP is positively related to the PECR.

H10. The implementation of CST programmes for employees and partners (SC key actors) is positively related to the PECR.

H11. The adoption of CRC strategies is positively related to the PECR.

H12. The adoption of CRI is positively related to the PECR.

The relationship between managers' perception of potential business interruption along the supply chain due to cyber risks and the PECR is mediated by the adoption of cyber resilience strategies. Thus, we built the following mediation hypotheses:

H13a. The relationship between PBIA and PECR is mediated by the adoption of CRGSP.

H13b. The relationship between PBIA and PECR is mediated by the implementation of CST programmes.

H13c. The relationship between PBIA and PECR is mediated by the adoption of CRC strategies.

H13d. The relationship between PBIA and PECR is mediated by the adoption of CRI.

H14a. The relationship between PRDA and PECR is mediated by the adoption of CRGSP.

H14b. The relationship between PRDA and PECR is mediated by the implementation of CST programmes.

H14c. The relationship between PRDA and PECR is mediated by the adoption of CRC strategies.

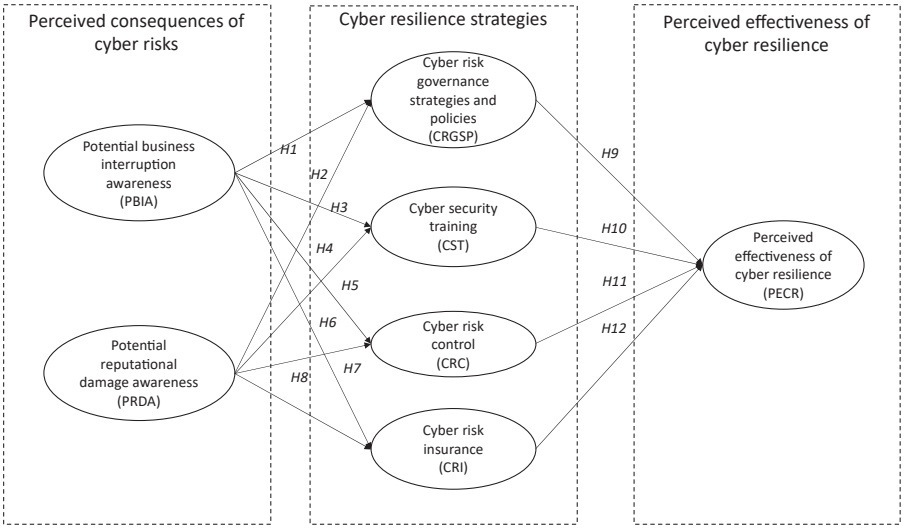
H14d. The relationship between PRDA and PECR is mediated by the adoption of CRI.

The conceptual model and the related hypotheses are summarised in Figure 1.

3. Research methodology

3.1 Survey and data collection

We used a survey to collect the perceptions of top managers at different levels of Italian organisations during the period 2021–2022. Following Kosutic and Pigni (2022), we gathered data from various functions, involving executive-level managers, SC managers/security managers, chief information officers, and risk managers, all of whom declared being key decision-makers for building cyber resilience strategies for their organisations. The organisations involved belong to different sectors: industrial sectors (55%), finance companies (29%), services organisations linked to SC management (14%), and others (2%). A pilot survey was conducted with a convenience sample of five managers from

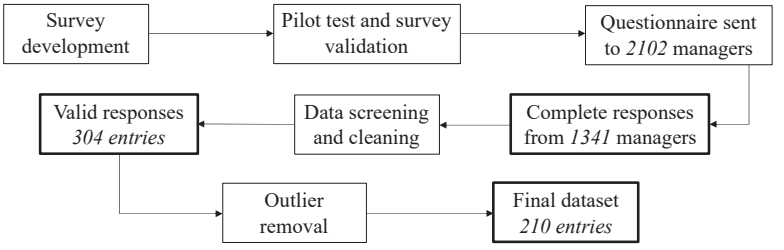


Source(s): Authors

Figure 1.
Conceptual model of cyber resilience

medium-sized and large organisations across various sectors to validate the questionnaire's comprehensibility and adequacy. This group included three managers from the industrial sectors and two from the finance and service sectors. Their feedback was instrumental in validating the questionnaire. Additionally, all participants confirmed that the questionnaire was well-suited to the key characteristics of their respective industries (Ghadge *et al.*, 2019).

Subsequently, the survey was created and administered through the survey provider, Qualtrics. We hired Qualtrics to identify suitable panels of practitioners, requiring target respondents to meet key criteria: their organisations had headquarters in Italy, and they held a managerial role in decision-making for building cyber resilience. Qualtrics contacted 2,102 panels according to the criteria, receiving complete responses from 1,341 managers, with a response rate of 63.8% (Figure 2). This high response rate may be unexpected, but it is because the survey provider partners with a wide list of subscribers. The data collected were subjected to a screening process. A total of 1,037 responses were removed based on three exclusion criteria (Abbey and Meloy, 2017): (1) respondents failed the attention checks; (2) disengaged participation as determined by excessive or too scarce completion time; and (3) respondents did not fall within the scope of the research. Furthermore, all the questionnaires



Source(s): Authors

Figure 2.
Phases of the survey development

collected were manually analysed to verify the completeness and consistency of the responses. The data-cleaning process resulted in 304 valid responses. We offered monetary incentives to all respondents who had their survey validated (Hong and Hales, 2023). Lastly, a Mahalanobis distance inspection was conducted to identify outliers (De Maesschalck *et al.*, 2000; Hawkins, 1980). A total of 94 outliers were detected and removed, resulting in a final dataset of 210 usable responses. Respondent and industry profiles are provided in Table 1.

3.2 Measures

The constructs of the theoretical model were developed building upon items previously measured in the context of cybersecurity (Eling and Wirfs, 2019; Ganin *et al.*, 2020; Garcia-Perez *et al.*, 2021; Hoppe *et al.*, 2021; Kanwal *et al.*, 2022; Li *et al.*, 2019; Öğüt *et al.*, 2011; Samhan, 2020). The process of construct definition has been supported and guided by the combination of several sources. The scale items for the constructs of awareness (of both PBIA and PRDA) were developed based on Yang *et al.* (2020) and with the support of Li *et al.* (2019) and Hoppe *et al.* (2021). The constructs of CRGSP, cyber security training, CRC, and PECR were developed primarily based on Kanwal *et al.* (2022), with the support of Ganin *et al.* (2020), Garcia-Perez *et al.* (2021) and Abraham *et al.* (2019). For CRI, we adapted Ogbanufe *et al.* (2021), with supporting literature from Samhan (2020). The pilot study pre-assessed the validity and reliability of the items. All variable scales were measured using a five-point Likert-type response (1 – Strongly Disagree, 5 – Strongly Agree) (Gonul Kochan *et al.*, 2016; Koh *et al.*, 2023; Uvet *et al.*, 2023). Table 2 summarises the constructs used in this study.

4. Data analysis and results

4.1 Model assessment

Data were analysed using structural equation modelling (SEM) to test the proposed hypotheses and conceptual model. IBM SPSS Amos 26 software (Arbuckle, 2019) was used.

Respondent profile	*N*	%	Industry profile	*N*	%
Gender			*Organization sector*		
Male	156	74	Industrial	115	55
Female	54	26	Finance	61	29
Age (in years)			Services	29	14
25–40	107	51	Other	5	2
41–60	99	47	*Organization size*		
>60	4	2	Small	48	23
Work experience (in years)			Medium	34	16
0–5	46	22	Large	128	61
6–10	62	30			
>10	102	49			
Educational qualification					
Degree	138	66			
Diploma	59	28			
PhD	11	5			
Middle school diploma	2	1			
Role					
Executive level member	44	21			
Manager (SC/security)	121	57			
Chief information officer/Risk manager	45	22			

Source(s): Authors

Table 1. Respondents and industry profile

Constructs	Measurement items	Adapted source
Potential Business Interruption Awareness (PBIA)	I am updated in terms of threats related to business interruption (PBIA1) I understand the risk of incidents related to business interruption (PBIA2)	Yang *et al.* (2020)
Potential Reputational Damage Awareness (PRDA)	I am updated in terms of threats related to reputation damage (PRDA1) I understand the risk of incidents related to reputation damage (PRDA2)	Yang *et al.* (2020)
Cyber Risk Governance Strategies and Policies (CRGSP)	Our (investments in) policies are clear and appropriate (CRGSP1) Our (investments in) procedures cover all the aspects of cyber risk in accordance with the required regulations (CRGSP2) Our (investments in) procedures are reviewed and updated for addressing new vulnerabilities (CRGSP3)	Kanwal *et al.* (2022)
Cyber Security Training (CST)	Our organisation regularly holds training programme for employees (CST1) Training that is carried out by our organisation covers critical aspects of cyber risk (CST2)	Kanwal *et al.* (2022)
Cyber Risk Control (CRC)	Our (investments in) IT and OT systems/equipment are deigned and maintained to provide maximum protection (CRC1) The software for the systems is kept up to date (CRC2)	Kanwal *et al.* (2022)
Cyber Risk Insurance (CRI)	My organisation is committed to supporting efforts in adopting cyber risk insurance for managing cyber risks (CRI1) The use of cyber risk insurance for managing cyber risks is important to our organisation (CRI2)	Ogbanufe *et al.* (2021)
Perceived Effectiveness of Cyber Resilience (PECR)	Cyber risk (strategies) implementation can largely improve performances (cyber resilience) (PECR1) Our organisation (invests) in effective measures to remain operational even if we lose access to a critical digital asset (PECR2)	Kanwal *et al.* (2022)

Source(s): Authors

Table 2. Constructs

First, we checked for survey non-response bias and common method bias. Then, we checked for reliability, convergent validity, and discriminant validity. Subsequently, we estimated the measurement model and the structural model (Kline, 2011) under two separate SEM steps.

A non-response bias test was performed by conducting a Mann-Whitney U test to detect statistically significant differences between early respondents and late respondents as a proxy for non-respondents (Wagner and Kemmerling, 2010). The first quartile and last quartile of respondents did not reveal any statistically significant differences ($p < 0.05$), implying that non-response bias was not a significant concern for our data (Armstrong and Overton, 1977). Regarding the common method bias, we attempted to minimise it through the adoption of ex-ante procedural approaches (Podsakoff *et al.*, 2012). We assured the respondents of complete anonymity and confidentiality of their answers and assured them that there were no right or wrong answers. This procedure also allowed us to control and thereby minimise social desirability bias. We provided descriptions for potentially unfamiliar constructs and avoided complicated syntax to improve clarity. Survey

questions were not labelled with relevant theoretical constructs so that the respondents could not guess the underlying causal relationships (Hulland *et al.*, 2018). We further performed a post-hoc common latent factor test. A measurement model with and without the common latent factor was run to see the differences in the model fit parameters such as the Tucker-Lewis fit index (TLI) and comparative fit index (CFI) (Chavez *et al.*, 2023). The differences in the model fit parameters were marginally different (ΔTLI and ΔCFI <0.015), indicating that the common method was not a major issue in our data (Hulland *et al.*, 2018).

Table 3 summarises the results of the reliability, convergent validity, and discriminant validity estimates. To check for reliability and internal consistency, Cronbach's alpha and composite reliability (CR) were computed for each construct. The values of Cronbach's alpha were found to be acceptable, all higher than 0.7, except for one construct that had a slightly lower but still adequate alpha value. CR values ranging from 0.6 to 0.7 and above are good indicators of a latent variable's reliability (Sarstedt *et al.*, 2014).

For convergent validity to be observed, CR has to be higher than the average variance extracted (AVE), and the AVE is recommended to be higher than 0.5 (Hair *et al.*, 2014). The values observed in our analysis met these requirements. Therefore, the items effectively represent the related constructs—they are internally consistent and reliable in measuring them (Hair *et al.*, 2014).

For discriminant validity, the AVE for each latent construct is greater than the construct's highest squared correlation with any other latent variable. Thus, convergent and discriminant validity are accomplished (Fornell and Larcker, 1981). The results of the reliability and convergent validity analysis are in Table 3. Table 4 summarises the highest squared correlation between constructs.

Moreover, confirmatory factor analysis (CFA) was used to evaluate the measurement model. The overall goodness of fit was satisfactory. The ratio of the chi-squared and the degrees of freedom (CMIN/DF) was 2.09, below the threshold of 3 (Schumacker and Lomax, 2016). The CFI was 0.96, above the cutoff of 0.93 (Bagozzi and Yi, 2012). Finally, the root mean square error of approximation (RMSEA) was 0.072, which satisfies the upper limit threshold (Hooper *et al.*, 2008). Since the assessment of the validity of the measurement model provided satisfactory results, we proceeded with an estimation of the structural model to compute the path coefficients for the hypothesis testing.

Construct	Item	Cronbach's alpha	Loading	CR	AVE
PBIA	PBIA1	0.681	0.711	0.682	0.517
	PBIA2		0.727		
PRDA	PRDA1	0.734	0.91	0.758	0.617
	PRDA2		0.637		
CRGSP	CRGSP1	0.912	0.911	0.913	0.778
	CRGSP2		0.859		
	CRGSP3		0.876		
CST	CST1	0.880	0.837	0.883	0.791
	CST2		0.939		
CRC	CRC1	0.757	0.72	0.762	0.617
	CRC2		0.846		
CRI	CRI 1	0.842	0.806	0.845	0.733
	CRI 2		0.903		
PECR	PECR1	0.801	0.777	0.804	0.673
	PECR2		0.861		

Table 3.
Measurement model

Source(s): Authors

Lastly, we checked for potential differences among respondents based on the size and sector of their organisations through a cluster analysis. The quality threshold for coherence and separation of the clusters was not reached, indicating that the variables were not validated. This suggests that despite the highest availability of resources and more sophisticated cyber risk approaches in large-sized organisations (Ghadge *et al.*, 2019), the SMEs in our sample seem to offset the "size effect" with their awareness of cyber resilience and commitment to cyber resilience capabilities and strategies. This evidence allows us to enrich the results of the study by Colicchia *et al.* (2019).

Moreover, our analysis revealed that the organisations' sectors did not serve as a significant differentiator among respondents. This finding implies that the approach to cyber resilience is broadly similar across different sectors. Regardless of the specific sector, organisations appear to be equally committed to and aware of the importance of cyber resilience, highlighting a broad recognition of the need to effectively address cyber risks. This underscores the relevance and applicability of our findings across diverse industries, reinforcing the notion that effective cyber resilience strategies are not sector-specific but broadly applicable.

4.2 The structural model: direct effects

After assessing the validity of the measurement model, we proceeded with the estimation of the structural model. The indices of fit showed that the structural model matched the data satisfactorily. The CMIN/DF ratio was below the threshold of 3 (=2.73) (Kline, 2011). Moreover, the RMSEA value of 0.083 indicated a satisfactory model fit (Gerbing and Anderson, 1992), and the CFI was above the cutoff of 0.93 (=0.95) (Bagozzi and Yi, 2012). The results of the structural model estimation are summarised in Table 5.

We found that potential business interruption awareness due to cyber risks triggered investment in the four strategies. Similarly, potential reputational damage awareness due to cyber risks drove investments in three of the four strategies, excluding risk control strategies, as explained below.

We found that PBIA, due to cyber risks, positively influenced the adoption of all four cyber resilience strategies. The direct effect was found to be statistically significant ($p < 0.001$). Therefore, the hypotheses H1, H3, H5, and H7 are supported. Moreover, the direct and positive effect of PRDA due to cyber risks on the adoption of the cyber resilience strategies was confirmed ($p < 0.05$), except for the CRC strategy. Thus, the hypotheses H2, H4, and H8 are confirmed, whereas the hypothesis H6 is not supported ($p > 0.05$).

Surprisingly, our results showed that the PECR is positively influenced by only two cyber resilience strategies: cyber risk governance strategies and cyber security training. Our analysis of whether the adoption of the cyber resilience strategies is positively related to the PECR in SC management revealed that only the implementation of CRGSP and CST

	PBIA	PRDA	CRGSP	CST	CRC	CRI	PECR
PBIA	0.266						
PRDA	0.162	0.335					
CRGSP	0.305	0.109	0.651				
CST	0.207	0.101	0.392	0.618			
CRC	0.166	0.071	0.458	0.300	0.371		
CRI	0.279	0.084	0.325	0.360	0.348	0.530	
PECR	0.190	0.049	0.394	0.530	0.274	0.373	0.446

Source(s): Authors

Table 4. The highest squared correlation between constructs

Structural effects			Standardized coefficient	SE
PBIA	→	CRGSP	0.883***	0.207
PRDA	→	CRGSP	0.149*	0.076
PBIA	→	CST	0.74***	0.222
PRDA	→	CST	0.207*	0.108
PBIA	→	CRC	0.909***	0.189
PRDA	→	CRC	0.13	0.063
PBIA	→	CRI	0.787***	0.211
PRDA	→	CRI	0.16*	0.083
CRGSP	→	PECR	0.485*	0.18
CST	→	PECR	0.605***	0.081
CRC	→	PECR	−0.13	0.315
CRI	→	PECR	0.235	0.104
PBIA	→	PECR	−0.126	0.883
PRDA	→	PECR	−0.139	0.1

Table 5.
Structural model results

Note(s): Significance levels: *$p < 0.05$; **$p < 0.01$; ***$p < 0.001$ (two-tailed test); t-value = 1.96
Source(s): Authors

positively and significantly influenced PECR. Hence, hypotheses H9 and H10 are supported ($p < 0.001$, $p < 0.05$). The adoption of CRC or CRI strategies did not statistically influence PECR. Hence, hypotheses H11 and H12 are not supported ($p > 0.05$).

The statistically significant relations, as resulting from the structural model analysis, are highlighted in Figure 3.

4.3 The structural model: indirect effects

We performed an analysis of the indirect effects of our model (Table 4). The results confirmed our preliminary findings by revealing significant indirect effects, particularly of PBIA on PECR, when considering either the CRGSP or the CST cyber resilience strategies (De Oliveira *et al.*, 2023). Thus, the hypotheses H13a and H13b are confirmed.

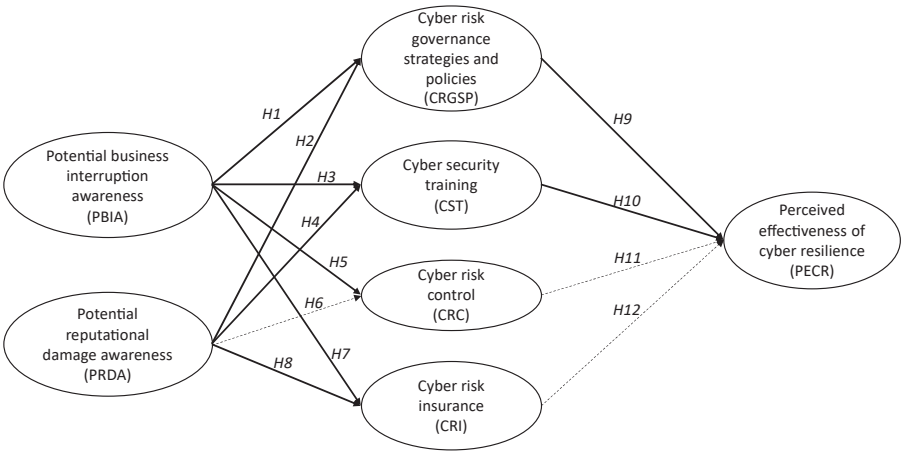


Figure 3.
Supported hypotheses

Source(s): Authors

The indirect effect analysis of PBIA/PRDA (independent variable) on PECR (dependent variable) mediated by the cyber resilience strategies was based on Baron and Kenny's (1986) study. The mediation analysis decomposes the total effect of a relationship between an independent and a dependent variable into direct and indirect impacts influenced by a mediator of such a relationship. To verify the existence of a mediation relationship, they recommended the following steps: (1) verify if the independent variable significantly and directly affects the mediating variable; (2) check if the independent variable significantly affects the dependent variable in the absence of the mediator; (3) determine if the mediator variable significantly affects the dependent variable; and (4) verify if the impact of the independent variable on the dependent one decreases in the presence of the mediator in the model. Partial mediation exists when the impact is reduced but still significant, while full mediation exists if the effect is no longer significant. We ran all steps for each independent variable, considering each mediator variable. Table 6 presents the steps and the results of the mediation test. We observed that only the CRGSP and CST strategies fully mediated the relationship between PBIA and PECR, whereas the other two strategies did not significantly mediate. Furthermore, no significant indirect effect of PRDA was observed on PECR. The significant indirect effects are further depicted in Figure 4 with a continuous line, whereas the dotted lines represent the indirect relationship not statistically significant.

Additionally, the Sobel (1987) statistical test was used to test the significance of the indirect effect, where applicable (De Oliveira *et al.*, 2023). The analysis confirmed the significance of the effect, showing values greater than the cutoff of 1.96 and $p < 0.05$ (Table 6) (Sobel, 1987).

5. Discussion and conclusion

According to the TPR (Jia *et al.*, 1999), our results show that managers' perceptions about the expected negative consequences of cyber risks drive their decisions to implement cyber resilience strategies.

In a dynamic path in line with the DCT, the implementation of cyber resilience strategies moves from an initial (subjective) managerial awareness of the cyber threat and the assessment of potential damages to the strategic investments and finally to the perceived effectiveness (subjectively again) of the existing protection against future cyber threats.

The first clear evidence is that organisations must invest in their dynamic capabilities to detect fast-changing cyber threats, properly assess vulnerabilities, and evaluate potential loss exposure to build effective managerial paths towards cyber resilience. This finding is strongly supported by existing research and guidelines. Additionally, this study provides original contributions in three directions, detailed in the following sub-sections.

5.1 Cyber risks are perceived to mainly generate business interruption, and this is the trigger to invest in protecting the organisation

Our findings reveal how different managerial perceptions about the consequences of cyber risks (Jia *et al.*, 1999)—specifically in terms of business interruption along the supply chain and/or reputational damage—lead to the implementation of specific portfolios of cyber resilience strategies. These strategies, in turn, influence the PECR.

The PECR might then affect the perception of risk exposure, creating a continuous cycle that could prompt further strategic investments.

Our study indicates that, given the two different potential negative effects of cyber risks (De Gusmão *et al.*, 2018; Carnovale and Yeniyut, 2021), managers exhibit a higher sensitivity towards the threat of business interruption along the supply chain. This awareness drives a strong commitment to implementing a comprehensive mix of cyber resilience strategies, aligning with the theoretical frameworks proposed by Ram and Zhang (2020) and Ivanov (2022).

Hypothesis	Steps	Relationship between constructs	Standardized coefficients	p-value	Sobel test
H13a	1	PBIA → CRGSP	0.883	<0.001	2.278
	2	PBIA → PECR*	0.628	<0.001	(p = 0.0227)
	3	CRGSP → PECR	0.485	<0.05	
	4	PBIA → PECR**	−0.126	= 0.836	
H13b	1	PBIA → CST	0.74	<0.001	3.044
	2	PBIA → PECR*	0.628	<0.001	(p = 0.0023)
	3	CST → PECR	0.605	<0.001	
	4	PBIA → PECR**	−0.126	= 0.836	
H13c	1	PBIA → CRC	0.909	<0.001	No indirect
	2	PBIA → PECR*	0.628	<0.001	effect
	3	CRC → PECR	−0.13	= 0.68	
	4	PBIA → PECR**	−0.126	= 0.836	
H13d	1	PBIA → CRI	0.787	<0.001	No indirect
	2	PBIA → PECR*	0.628	<0.001	effect
	3	CRI → PECR	0.235	= 0.074	
	4	PBIA → PECR**	−0.126	= 0.836	
H14a	1	PRDA → CRGSP	0.149	<0.05	No indirect
	2	PRDA → PECR*	0.138	= 0.117	effect
	3	CRGSP → PECR	0.485	<0.05	
	4	PRDA → PECR**	−0.139	= 0.254	
H14b	1	PRDA → CST	0.207	<0.05	No indirect
	2	PRDA → PECR*	0.138	= 0.117	effect
	3	CST → PECR	0.605	<0.001	
	4	PRDA → PECR**	−0.139	= 0.254	
H14c	1	PRDA → CRC	0.13	= 0.092	No indirect
	2	PRDA → PECR*	0.138	= 0.117	effect
	3	CRC → PECR	−0.13	= 0.68	
	4	PRDA → PECR**	−0.139	= 0.254	
H14d	1	PRDA → CRI	0.16	<0.05	No indirect
	2	PRDA → PECR*	0.138	= 0.117	effect
	3	CRI → PECR	0.235	= 0.074	
	4	PRDA → PECR**	−0.139	= 0.254	

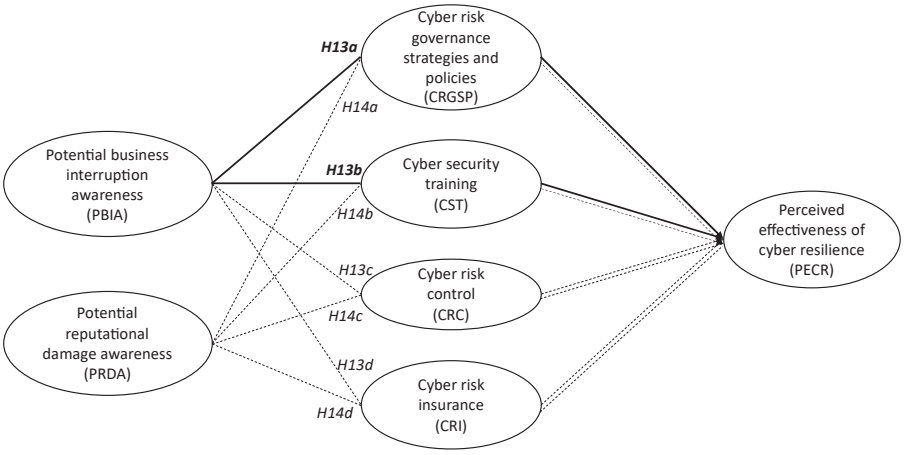
Table 6.
Cyber resilience strategies mediation test

Note(s): *Relationship between the independent variable (PBIA or PRDA) and PECR without cyber resilience strategy mediator; **Relationship between the independent variable (PBIA or PRDA) and PECR with cyber resilience strategy mediator
Source(s): Authors

Surprisingly, managers are less sensitive to reputational damage as a potential consequence of cyber threats. Thus, reputation is not the primary trigger for investing in CRC. This finding seems to complete and enrich part of the literature that emphasises reputation as a key asset to protect against emergent risks (Colicchia *et al.*, 2019). Our study highlights that the level of awareness regarding reputational damages is still very low. This underscores the importance of building appropriate awareness about when and how cyber threats can compromise valuable organisational assets and how these perceptions drive the implementation of cyber resilience strategies.

5.2 Cyber resilience strategies are differently perceived and adopted

Most existing frameworks and guidelines recommend investing in the entire portfolio of cyber resilience strategies. However, many authors note that investments remain inadequate without detailing the paths of investments, the propensity, or the willingness to adopt each strategy (Kanwal *et al.*, 2022).



Source(s): Authors

Figure 4.
Significant indirect effects

The novelty of this study lies in highlighting how managers can configure the mix of adopted cyber resilience strategies differently based on their perception of the potential negative consequences of cyber risks. This approach makes the entire cyber resilience management model more customised and influenced by the decision-makers' level of awareness, according to TPR. Our findings show that varying levels of managerial awareness lead to the implementation of different cyber resilience strategies. When corporate reputation is at risk, managers tend to focus more on managing cyber threats from a managerial perspective rather than employing physical risk control strategies. Conversely, when managers are aware of potential business interruption along the supply chain due to a cyberattack, there is a strong commitment to all the cyber resilience strategies. This finding partially contradicts Samhan's (2020) results, which addressed the effectiveness of cyber resilience investments in general, independent of the perceived negative impacts resulting from cyber incidents.

5.3 Cyber resilience capabilities as antecedents to develop effective cyber resilience strategies

Organisations must bridge the gap between managers' perceptions of cyber risk consequences, effective investments in cyber resilience strategies, the concrete configurations of dynamic capabilities related to these strategies, and the effectiveness of cyber resilience (Friday *et al.*, 2024).

Our results confirm that organisations can choose different paths for implementing their cyber resilience strategies (Schilke, 2014), as the four strategies can be configured differently. To effectively implement these strategies, managers should focus on the antecedents inherent in their related capabilities, as emphasised by Teece *et al.* (2016). Given the scarcity of studies on cyber resilience and related dynamic capabilities in SCs, we draw on key evidence from our study to offer future research directions and provide practitioners with insights for practical cyber resilience implementation.

For the first significant cyber resilience strategy included in our analysis, CRGSP, organisations must develop strategic capabilities and approaches to establish governance and policy models to address cyber threats (Teece *et al.*, 2016). Each organization should cultivate its dynamic capabilities to develop tailored approaches to cyber risk governance, focussing on specific legal requirements, digital capabilities, and human resources (Dubey *et al.*, 2023). Furthermore, considering the rapidly changing legal landscape and evolving

cyber threats, organisations must exercise and enhance their dynamic capabilities to achieve effective governance for cyber resilience.

CST remains a relevant cyber resilience strategy, highlighting the importance of developing capabilities related to the learning perspective and knowledge management tailored to the needs of specific firms (Easterby-Smith and Prieto, 2008). Managers should understand the potential pathways for developing the learning and training perspective from a DC standpoint to practically implement cultural and managerial cyber resilience strategies for effective protection against cyber threats along the supply chain.

Despite the study's results, it is crucial in the future to support managers in recognising the value of dynamic capabilities linked to CRC or CRI strategies. This can aid in constructing varied "dynamic response maps" against risks (Arena *et al.*, 2013) and creating ad-hoc portfolios of insurance programmes (Stechemesser *et al.*, 2015).

Additionally, our study identifies a stronger path towards cyber resilience: decision-makers' perception of business interruption along the supply chain as a significant negative consequence of cyber risks leads to prioritised investments in CRGSP and CST programmes.

The study also highlights the importance of exploring subjective perceptions of critical risks and corresponding measures of loss exposure (Baghersad and Zobel, 2022; Jia *et al.*, 1999), particularly for novel risks such as cyber risks that are challenging to detect early and measure accurately.

5.4 Theoretical implications

According to the TPR (Jia *et al.*, 1999), perceived risk consequences depend on the subjective understanding of the expected losses linked to a risk manifestation. This awareness influences decision-makers' choices regarding risk mitigation strategies (Wang *et al.*, 2013). The study extends the TPR by demonstrating that different managerial perceptions of risk lead to varying risk prevention and mitigation investments. This contrasts with existing literature that typically conceptualises a unique relationship between risk perception and specific mitigation actions. For instance, Yang *et al.* (2020) investigated how stakeholders' awareness influenced the intention of firms to invest in information disclosure quality and governance models, while Garcia-Perez *et al.* (2021) examined how risk perception guided cybersecurity investments. Moving a step further, our study indicates that different managerial perceptions of risks related to expected losses influence risk prevention and mitigation investments, offering significant insights for future research on risk management strategies among different supply chain actors.

The study integrates the DC perspective to analyse the PECR strategies within SCs. It underscores the need to continuously improve the knowledge and dynamic capabilities that managers must implement within evolving cyber risk scenarios (Teece *et al.*, 2016). This study offers an original investigation because, although a few cyber resilience studies have adopted the dynamic capability perspective (Ferdinand, 2015; Kosutic and Pigni, 2022; Teece *et al.*, 2016), it has not been extensively investigated in empirical studies. The research shows how dynamic capabilities such as strategic decision-making and resource reconfiguration are crucial for developing effective cyber resilience strategies. This contributes to the literature by linking dynamic capabilities directly with cyber resilience, offering a framework for how organisations can dynamically adapt to evolving cyber threats.

Moreover, the DC perspective sheds light on the importance of the antecedents of cyber resilience strategies, which are inherently represented by their related capabilities. Different configurations of strategies and antecedents, viewed dynamically, can drive the organisation towards its goal (Fainshmidt *et al.*, 2016, 2019). Future research should link the four cyber resilience strategies to their respective dynamic capabilities, particularly those related to the "strategic sense-making capacity" of each firm and industry (Li and Liu, 2014).

This research is one of the few that investigates cyber risks and cyber resilience concerning business interruption from an SC perspective. Cyber risks have emerged as significant SC threats in recent years due to the increasingly digitalised and interconnected business environment (Ivanov, 2022; Colicchia *et al.*, 2019). Unlike many studies that focus on specific sectors or functions (Rehman and Ali, 2021; Wirtz and Weyerer, 2017; Abraham *et al.*, 2019), this research includes insights from managers across different functions (executive, supply chain, risk, and IT) and various industries. This broader perspective enhances the generalisability of the findings and underscores the importance of cross-functional collaboration in cyber resilience. It suggests that diverse managerial perspectives and collaborative efforts are essential for developing comprehensive and effective cyber risk strategies.

Finally, the study offers a comprehensive theoretical framework that links risk perception, mitigation strategies, and the perceived effectiveness of these strategies within SCs. This framework can be refined and tested in future research, providing a foundation for further theoretical development in the fields of SCRES and SCRM. By addressing the iterative process of risk perception and strategy adjustment, the study provides a dynamic view of cyber risk management that is more reflective of real-world conditions of the fast and ever-changing threats of cyber risks (Kosutic and Pigni, 2022).

5.5 Managerial implications

This research offers valuable insights for practitioners. First, it addresses one of the major challenges that organisations and SCs are currently facing in this era of digital transformation. The respondents of the study are managers at different levels and from various functions—executive, SC, risk, and IT—who serve as the "key experts" on the topic of cyber resilience in their organisations (Eling and Schnell, 2016; Eling and Wirfs, 2019). Most existing studies and frameworks typically involve only IT and security managers as key decision-makers in defining the cyber risk mitigation strategy (Rehman and Ali, 2021; De Gusmão *et al.*, 2018; Diesch *et al.*, 2020). Therefore, we propose a broader perspective that includes managers from multiple functions to define a more comprehensive and effective cyber resilience strategy. Involving managers from different functions is crucial because it ensures that various perspectives and expertise are integrated into the strategy. The managerial implications of this approach are significant. It encourages cross-functional collaboration, enhances the understanding of cyber risks across departments, and fosters a culture of shared responsibility for cybersecurity. This inclusive strategy strengthens the organisation's overall and supply chain cyber resilience and ensures that all critical functions are prepared to respond to and recover from cyber threats effectively.

Despite the extensive literature on guidelines and frameworks for cyber resilience, this study helps organisations bridge the gap between their risk perceptions, investments in cyber risk management strategies, and overall cyber resilience. Whether or not certain cyber resilience strategies have already been implemented or are perceived as relevant, the crucial point is to conduct a thoughtful evaluation of the potential consequences of cyber risks and to make dynamic investments in resilience capabilities that can lead to effective strategies. Different configurations of strategies are inherently subjective, but firms must define their own paths towards a dynamic risk resilience map, as supported by the DC perspective (Arena *et al.*, 2013). Dynamic capabilities for cyber resilience include "specific strategic and organisational processes like (. . .) strategic decision making that create value for firms within dynamic markets by manipulating resources into new value-creating strategies" (Eisenhardt and Martin, 2000, p. 1106). Therefore, organisations can assess their needs in terms of cyber risks and dynamically develop their own cyber risk capabilities and strategies.

5.6 Research limitations and future research direction

Even though the study is grounded in literature and the analysis has been rigorously conducted, it is not without limitations. First, our empirical evidence is based on a sample of Italian companies. Future research should include companies from different countries to determine if and how the results might be country-specific. Furthermore, the survey data were gathered within a limited timeframe, suggesting two potential avenues for further research: conducting longitudinal studies over several periods or examining a single organisation's dynamic cycle of cyber risk perception and investments in cyber resilience strategies along the supply chain. This would involve an ongoing reassessment of risk perception and the implementation of resilience strategies. Additionally, while we employed SEM for our analysis, other methodologies could also be used. Future research could adopt different approaches such as mixed methods to validate and extend our findings. Moreover, our study focuses on the evaluation of perceived negative consequences of cyber risks, while other measures were not considered. Future research should include other metrics of cyber risks and investigate if and how these perceived negative consequences materialise, impacting areas such as supply chain value creation (Petratos, 2021; Salimath and Philip, 2020).

References

Abbey, J.D. and Meloy, M.G. (2017), "Attention by design: using attention checks to detect inattentive respondents and improve data quality", *Journal of Operations Management*, Vols 53-56 No. 1, pp. 63-70, doi: 10.1016/j.jom.2017.06.001.

Abraham, C., Chatterjee, D. and Sims, R.R. (2019), "Muddling through cybersecurity: insights from the US healthcare industry", *Business Horizons*, Vol. 62 No. 4, pp. 539-548, doi: 10.1016/j.bushor.2019.03.010.

Allianz (Ed.) (2023), *Allianz Risk Barometer: Top 10 Global Business Risks for 2022*, available at: https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2023-press.html

Arbuckle, J.L. (2019), *Amos*, (Version 26.0) [Computer Program], IBM SPSS, Chicago.

Arcuri, M.C., Gai, L., Ielasi, F. and Ventisette, E. (2020), "Cyber attacks on hospitality sector: stock market reaction", *Journal of Hospitality and Tourism Technology*, Vol. 11 No. 2, pp. 277-290, doi: 10.1108/jhtt-05-2019-0080.

Arena, M., Azzonea, G., Cagno, E., Ferrettia, G., Prunotto, E., Silvestri, A. and Trucco, P. (2013), "Integrated risk management through dynamic capabilities within project-based organizations: the company dynamic response map", *Risk Management*, Vol. 15 No. 1, pp. 50-77, doi: 10.1057/rm.2012.12.

Armstrong, J.S. and Overton, T.S. (1977), "Estimating nonresponse bias in mail surveys", *Journal of Marketing Research*, Vol. 14 No. 3, pp. 396-402, doi: 10.2307/3150783.

Baghersad, M. and Zobel, C.W. (2022), "Organizational resilience to disruption risks: developing metrics and testing effectiveness of operational strategies", *Risk Analysis*, Vol. 42 No. 3, pp. 561-579, doi: 10.1111/risa.13769.

Bagozzi, R.P. and Yi, Y. (2012), "Specification, evaluation, and interpretation of structural equation models", *Journal of the Academy of Marketing Science*, Vol. 40 No. 1, pp. 8-34, doi: 10.1007/s11747-011-0278-x.

Baron, R.M. and Kenny, D.A. (1986), "The moderator-mediator variable distinction in social psychological research: conceptual, strategic, and statistical considerations", *Journal of Personality and Social Psychology*, Vol. 51 No. 6, pp. 1173-1182, doi: 10.1037/0022-3514.51.6.1173.

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, doi: 10.1016/j.technovation.2014.01.005.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, Vol. 34 No. 3, pp. 523-548, doi: 10.2307/25750690.

Burt, A. (2019), *Cybersecurity Is Putting Customer Trust at the Center of Competition*, available at: https://hbr.org/2019/03/cybersecurity-is-putting-customer-trust-at-the-center-of-competition

Camillo, M. (2017), "Cyber risk and the changing role of insurance", *Journal of Cyber Policy*, Vol. 2 No. 1, pp. 53-63, doi: 10.1080/23738871.2017.1296878.

Carnovale, S. and Yeniyurt, S. (Eds) (2021), *Cyber Security and Supply Chain Management: Risks, Challenges, and Solutions*. World Scientific.

Chavez, R., Malik, M., Ghaderi, H. and Yu, W. (2023), "Environmental collaboration with suppliers and cost performance: exploring the contingency role of digital orientation from a circular economy perspective", *International Journal of Operations and Production Management*, Vol. 43 No. 4, pp. 651-675, doi: 10.1108/ijopm-01-2022-0072.

Christopher, M. and Peck, H. (2004), "Building the resilient supply chain", *International Journal of Logistics Management*, Vol. 15 No. 2, pp. 1-13, doi: 10.1108/09574090410700275.

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, doi: 10.1108/scm-09-2017-0289.

Collier, Z.A., Dimase, D., Walters, S., Tehranipoor, M.M., Lambert, J.H. and Linkov, I. (2014), "Cybersecurity standards: managing risk and creating resilience", *Computer*, Vol. 47 No. 9, pp. 70-76, doi: 10.1109/mc.2013.448.

Confente, I., Siciliano, G., Gaudenzi, B. and Eickhoff, M. (2019), "Effects of data breaches from user-generated content: a corporate reputation analysis", *European Management Journal*, Vol. 37 No. 4, pp. 492-504, doi: 10.1016/j.emj.2019.01.007.

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, doi: 10.1108/scm-02-2020-0073.

Culot, G., Nassimbeni, G., Podrecca, M. and Sartor, M. (2021), "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda", *The TQM Journal*, Vol. 33 No. 7, pp. 76-105, doi: 10.1108/tqm-09-2020-0202.

Davis, A. (2015), "Building cyber-resilience into supply chains", *Technology Innovation Management Review*, Vol. 5 No. 4, pp. 19-27, doi: 10.22215/timreview887.

De Gusmão, A.P.H., Silva, M.M., Poleto, T., Silva, L.C.E. and Costa, A.P.C.S. (2018), "Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory", *International Journal of Information Management*, Vol. 43, pp. 248-260, doi: 10.1016/j.ijinfomgt.2018.08.008.

De Maesschalck, R., Jouan-Rimbaud, D. and Massart, D.L. (2000), "The Mahalanobis distance", *Chemometrics and Intelligent Laboratory Systems*, Vol. 50 No. 1, pp. 1-18, doi: 10.1016/s0169-7439(99)00047-7.

De Oliveira, A.S., Souki, G.Q., Da Silva, D., Silva, M.A.R. and Medeiros, F.D.A.D.S. (2023), "Impacts of service guarantees on consumers' perceived quality and satisfaction in e-commerce", *International Journal of Quality and Reliability Management*, Vol. 40 No. 10, pp. 2559-2580, doi: 10.1108/ijqrm-06-2022-0175.

Diesch, R., Pfaff, M. and Krcmar, H. (2020), "A comprehensive model of information security factors for decision-makers", *Computers and Security*, Vol. 92, 101747, doi: 10.1016/j.cose.2020.101747.

Dubey, R., Bryde, D.J., Dwivedi, Y.K., Graham, G., Foropon, C. and Papadopoulos, T. (2023), "Dynamic digital capabilities and supply chain resilience: the role of government effectiveness", *International Journal of Production Economics*, Vol. 258, 108790, doi: 10.1016/j.ijpe.2023.108790.

Easterby-Smith, M. and Prieto, I.M. (2008), "Dynamic capabilities and knowledge management: an integrative role for learning?", *British Journal of Management*, Vol. 19 No. 3, pp. 235-249.

Eisenhardt, K.M. and Martin, J.A. (2000), "Dynamic capabilities: what are they?", *Strategic Management Journal*, Vol. 21 Nos 10-11, pp. 1105-1121, doi: 10.1002/1097-0266(200010/11)21:10/11<1105::aid-smj133>3.0.co;2-e.

Eling, M. and Schnell, W. (2016), "What do we know about cyber risk and cyber risk insurance?", *The Journal of Risk Finance*, Vol. 17 No. 5, pp. 474-491, doi: 10.1108/jrf-09-2016-0122.

Eling, M. and Wirfs, J. (2019), "What are the actual costs of cyber risk events?", *European Journal of Operational Research*, Vol. 272 No. 3, pp. 1109-1119, doi: 10.1016/j.ejor.2018.07.021.

Fainshmidt, S., Pezeshkan, A., Lance Frazier, M., Nair, A. and Markowski, E. (2016), "Dynamic capabilities and organizational performance: a meta-analytic evaluation and extension", *Journal of Management Studies*, Vol. 53 No. 8, pp. 1348-1380, doi: 10.1111/joms.12213.

Fainshmidt, S., Wenger, L., Pezeshkan, A. and Mallon, M.R. (2019), "When do dynamic capabilities lead to competitive advantage? The importance of strategic fit", *Journal of Management Studies*, Vol. 56 No. 4, pp. 758-787, doi: 10.1111/joms.12415.

Fan, Y. and Stevenson, M. (2018), "A review of supply chain risk management: definition, theory, and research agenda", *International Journal of Physical Distribution and Logistics Management*, Vol. 48 No. 3, pp. 205-230, doi: 10.1108/ijpdlm-01-2017-0043.

Ferdinand, J. (2015), "Building organisational cyber resilience: a strategic knowledge-based view of cyber security management", *Journal of Business Continuity and Emergency Planning*, Vol. 9 No. 2, pp. 185-195, doi: 10.69554/prjy4917.

Fornell, C. and Larcker, D.F. (1981), "Evaluating structural equation models with unobservable variables and measurement error", *Journal of Marketing Research*, Vol. 18 No. 1, pp. 39-50, doi: 10.2307/3151312.

Friday, D., Melnyk, S.A., Altman, M., Harrison, N. and Ryan, S. (2024), "An inductive analysis of collaborative cybersecurity management capabilities, relational antecedents and supply chain cybersecurity parameters", *International Journal of Physical Distribution and Logistics Management*, Vol. 54 No. 5, pp. 476-500, doi: 10.1108/ijpdlm-01-2023-0034.

Ganin, A.A., Quach, P., Panwar, M., Collier, Z.A., Keisler, J.M., Marchese, D. and Linkov, I. (2020), "Multicriteria decision framework for cybersecurity risk assessment and management", *Risk Analysis*, Vol. 40 No. 1, pp. 183-199, doi: 10.1111/risa.12891.

Garcia-Perez, A., Sallos, M.P. and Tiwasing, P. (2021), "Dimensions of cybersecurity performance and crisis response in critical infrastructure organisations: an intellectual capital perspective", *Journal of Intellectual Capital*, Vol. 24 No. 2, pp. 465-486, doi: 10.1108/jic-06-2021-0166.

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. 97-111, doi: 10.1108/scm-09-2022-0383.

Gerbing, D.W. and Anderson, J.C. (1992), "Monte Carlo evaluations of goodness of fit indices for structural equation models", *Sociological Methods and Research*, Vol. 21 No. 2, pp. 132-160, doi: 10.1177/0049124192021002002.

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, doi: 10.1108/scm-10-2018-0357.

Gonul Kochan, C., Pourreza, S., Tran, H. and Prybutok, V.R. (2016), "Determinants and logistics of e-waste recycling", *International Journal of Logistics Management*, Vol. 27 No. 1, pp. 52-70, doi: 10.1108/ijlm-02-2014-0021.

Grewal, D., Gotlieb, J. and Marmorstein, H. (1994), "The moderating effects of message framing and source credibility on the price-perceived risk relationship", *Journal of Consumer Research*, Vol. 21 No. 1, pp. 145-153, doi: 10.1086/209388.

Hair, J.F., Jr, Black, W.C., Babin, B.J. and Anderson, R.E. (2014), *Multivariate Data Analysis*, Pearson Education, Harlow, UK.

Hawkins, D.M. (1980), *Identification of Outliers*, Chapman & Hall, London, Vol. 11.

Heckmann, I., Comes, T. and Nickel, S. (2015), "A critical review on supply chain risk–definition, measure and modeling", *Omega*, Vol. 52, pp. 119-132, doi: 10.1016/j.omega.2014.10.004.

Hong, L. and Hales, D.N. (2023), "How blockchain manages supply chain risks: evidence from Indian manufacturing companies", *International Journal of Logistics Management*, Vol. 35 No. 5, pp. 1604-1627, doi: 10.1108/ijlm-05-2023-0178.

Hooper, D., Coughlan, J. and Mullen, M.R. (2008), "Structural equation modelling: guidelines for determining model fit", *Electronic Journal of Business Research Methods*, Vol. 6 No. 1, pp. 53-60.

Hoppe, F., Gatzert, N. and Gruner, P. (2021), "Cyber risk management in SMEs: insights from industry surveys", *The Journal of Risk Finance*, Vol. 22 Nos 3/4, pp. 240-260, doi: 10.1108/jrf-02-2020-0024.

Hulland, J., Baumgartner, H. and Smith, K.M. (2018), "Marketing survey research best practices: evidence and recommendations from a review of JAMS articles", *Journal of the Academy of Marketing Science*, Vol. 46 No. 1, pp. 92-108, doi: 10.1007/s11747-017-0532-y.

Ivanov, D. (2022), "Lean resilience: AURA (active usage of resilience assets) framework for post-COVID-19 supply chain management", *International Journal of Logistics Management*, Vol. 33 No. 4, pp. 1196-1217, doi: 10.1108/ijlm-11-2020-0448.

Ivanov, D. and Dolgui, A. (2020), "A digital supply chain twin for managing the disruption risks and resilience in the era of industry 4.0", *Production Planning and Control*, Vol. 32 No. 9, pp. 1-14, doi: 10.1080/09537287.2020.1768450.

Jia, J., Dyer, J.S. and Butler, J.C. (1999), "Measures of perceived risk", *Management Science*, Vol. 45 No. 4, pp. 519-532, doi: 10.1287/mnsc.45.4.519.

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, doi: 10.1108/13598541111139062.

Kanwal, K., Shi, W., Kontovas, C., Yang, Z. and Chang, C.H. (2022), "Maritime cybersecurity: are onboard systems ready?", *Maritime Policy and Management*, Vol. 51 No. 3, pp. 1-19, doi: 10.1080/03088839.2022.2124464.

Kline, R.B. (2011), *Principles and Practice of Structural Equation Modeling*, 3rd ed., Guilford, New York, NY.

Koh, L.Y., Peh, Y.S., Wang, X. and Yuen, K.F. (2023), "Adoption of online crowdsourced logistics during the pandemic: a consumer-based approach", *International Journal of Logistics Management*, Vol. 35 No. 2, pp. 531-556, doi: 10.1108/ijlm-05-2022-0213.

Kosutic, D. and Pigni, F. (2022), "Cybersecurity: investing for competitive outcomes", *Journal of Business Strategy*, Vol. 43 No. 1, pp. 28-36, doi: 10.1108/jbs-06-2020-0116.

Li, D.-Y. and Liu, J. (2014), "Dynamic capabilities, environmental dynamism, and competitive advantage: evidence from China", *Journal of Business Research*, Vol. 67 No. 1, pp. 2793-2799, doi: 10.1016/j.jbusres.2012.08.007.

Li, L., He, W., Xu, L., Ash, I., Anwar, M. and Yuan, X. (2019), "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behaviour", *International Journal of Information Management*, Vol. 45, pp. 13-24, doi: 10.1016/j.ijinfomgt.2018.10.017.

Maheshwari, P., Kamble, S., Kumar, S., Belhadi, A. and Gupta, S. (2023), "Digital twin-based warehouse management system: a theoretical toolbox for future research and applications", *International Journal of Logistics Management*, Vol. 35 No. 4, pp. 1073-1106, in press, doi: 10.1108/ijlm-01-2023-0030.

Marotta, A., Martinelli, F., Nanni, S., Orlando, A. and Yautsiukhin, A. (2017), "Cyber-insurance survey", *Computer Science Review*, Vol. 24, pp. 35-61, doi: 10.1016/j.cosrev.2017.01.001.

Mazzoccoli, A. and Naldi, M. (2020), "Robustness of optimal investment decisions in mixed insurance/investment cyber risk management", *Risk Analysis*, Vol. 40 No. 3, pp. 550-564, doi: 10.1111/risa.13416.

Meland, P.H., Tondel, I.A. and Solhaug, B. (2015), "Mitigating risk with cyberinsurance", *IEEE Security and Privacy*, Vol. 13 No. 6, pp. 38-43, doi: 10.1109/msp.2015.137.

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, doi: 10.1080/00207543.2021.1984606.

Ogbanufe, O., Kim, D.J. and Jones, M.C. (2021), "Informing cybersecurity strategic commitment through top management perceptions: the role of institutional pressures", *Information and Management*, Vol. 58 No. 7, 103507, doi: 10.1016/j.im.2021.103507.

Öğüt, H., Raghunathan, S. and Menon, N. (2011), "Cyber security risk management: public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection", *Risk Analysis*, Vol. 31 No. 3, pp. 497-512, doi: 10.1111/j.1539-6924.2010.01478.x.

Perera, S., Jin, X., Maurushat, A. and Opoku, D.G.J. (2022), "Factors affecting reputational damage to organisations due to cyberattacks", *Informatics*, Vol. 9 No. 1, p. 28, doi: 10.3390/informatics9010028.

Petratos, P.N. (2021), "Misinformation, disinformation, and fake news: cyber risks to business", *Business Horizons*, Vol. 64 No. 6, pp. 736-774, doi: 10.1016/j.bushor.2021.07.012.

Podsakoff, P.M., MacKenzie, S.B. and Podsakoff, N.P. (2012), "Sources of method bias in social science research and recommendations on how to control it", *Annual Review of Psychology*, Vol. 63 No. 1, pp. 539-569, doi: 10.1146/annurev-psych-120710-100452.

Protiviti (2023), *The Top Risks for 2023: A Global Perspective*, available at: https://www.protiviti.com/sites/default/files/2023-01/protiviti-newsletter-bp-issue159-top-risks-2023-global.pdf

Queiroz, M.M., Fosso Wamba, S. and Branski, R.M. (2022), "Supply chain resilience during the COVID-19: empirical evidence from an emerging economy", *Benchmarking: An International Journal*, Vol. 29 No. 6, pp. 1999-2018, doi: 10.1108/bij-08-2021-0454.

Queiroz, M.M., Fosso Wamba, S., Raut, R.D. and Pappas, I.O. (2023), "Does resilience matter for supply chain performance in disruptive crises with scarce resources?", *British Journal of Management*, Vol. 35 No. 2, pp. 974-991, doi: 10.1111/1467-8551.12748.

Ram, J. and Zhang, Z. (2020), "Belt and road initiative (BRI) supply chain risks: propositions and model development", *International Journal of Logistics Management*, Vol. 31 No. 4, pp. 777-799, doi: 10.1108/ijlm-12-2019-0366.

Rehman, Ou and Ali, Y. (2021), "Enhancing healthcare supply chain resilience: decision-making in a fuzzy environment", *International Journal of Logistics Management*, Vol. 33 No. 2, pp. 520-546, doi: 10.1108/ijlm-01-2021-0004.

Romanosky, S., Ablon, L., Kuehn, A. and Jones, T. (2019), "Content analysis of cyber insurance policies: how do carriers' price cyber risk?", *Journal of Cybersecurity*, Vol. 5 No. 1, p. tyz002, doi: 10.1093/cybsec/tyz002.

Safa, N.S., Von Solms, R. and Furnell, S. (2016), "Information security policy compliance model in organizations", *Computers and Security*, Vol. 56, pp. 70-82, doi: 10.1016/j.cose.2015.10.006.

Salimath, M.S. and Philip, J. (2020), "Cyber management and value creation: an organisational learning-based approach", *Knowledge Management Research and Practiceand*, Vol. 18 No. 4, pp. 474-487, doi: 10.1080/14778238.2020.1730719.

Samhan, B. (2020), "Can cyber risk management insurance mitigate healthcare providers' intentions to resist electronic medical records?", *International Journal of Healthcare Management*, Vol. 13 No. 1, pp. 12-21, doi: 10.1080/20479700.2017.1412558.

Sarstedt, M., Ringle, C.M., Smith, D., Reams, R. and Hair, Jr., J.F. (2014), "Partial least squares structural equation modeling (PLS-SEM): a useful tool for family business researchers", *Journal of Family Business Strategy*, Vol. 5 No. 1, pp. 105-115, doi: 10.1016/j.jfbs.2014.01.002.

Schilke, O. (2014), "On the contingent value of dynamic capabilities for competitive advantage: the nonlinear moderating effect of environmental dynamism", *Strategic Management Journal*, Vol. 35 No. 2, pp. 179-203, doi: 10.1002/smj.2099.

Schumacker, R.E. and Lomax, R.G. (2016), *A Beginner's Guide to Structural Equation Modeling*, 4th ed., Routledge, New York.

Singh, A., Gupta, M.P. and Ojha, A. (2014), "Identifying factors of 'organizational information security management", *Journal of Enterprise Information Management*, Vol. 27 No. 5, pp. 644-667, doi: 10.1108/jeim-07-2013-0052.

Sobel, M.E. (1987), "Direct and indirect effects in linear structural equation models", *Sociological Methods and Research*, Vol. 16 No. 1, pp. 155-176, doi: 10.1177/0049124187016001006.

Stallings, W. (2018), *Effective Cybersecurity: A Guide to Using Best Practices and Standards*, Addison-Wesley Professional, NJ.

Stechemesser, K., Endrikat, J., Grasshoff, N. and Edeltraud, G. (2015), "Insurance companies' responses to climate change: adaptation, dynamic capabilities and competitive advantage", *The Geneva Papers*, Vol. 40 No. 4, pp. 557-584, doi: 10.1057/gpp.2015.1.

Tambe, V., Bansod, G., Khurana, S. and Khandekar, S. (2022), "Reliability and availability of IoT devices in resource constrained environments", *International Journal of Quality and Reliability Management*, Vol. 39 No. 7, pp. 1648-1662, doi: 10.1108/ijqrm-09-2021-0334.

Taylor, J.W. (1974), "The role of risk in consumer behavior", *Journal of Marketing*, Vol. 38 No. 2, pp. 54-60, doi: 10.1177/002224297403800211.

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, doi: 10.1002/smj.640.

Teece, D.J., Pisano, G. and Shuen, A. (1977), "Dynamic capabilities and strategic management", *Strategic Management Journal*, Vol. 18 No. 7, pp. 509-533, doi: 10.1002/(sici)1097-0266(199708)18:7<509::aid-smj882>3.0.co;2-z.

Teece, D.J., 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, doi: 10.1525/cmr.2016.58.4.13.

Uvet, H., Dickens, J., Anderson, J., Glassburner, A. and Boone, C.A. (2023), "A hybrid e-logistics service quality approach: modeling the evolution of B2C e-commerce", *International Journal of Logistics Management*, Vol. 35 No. 4, pp. 1303-1331, doi: 10.1108/ijlm-06-2023-0238.

Wagner, S.M. and Kemmerling, R. (2010), "Handling nonresponse in logistics research", *Journal of Business Logistics*, Vol. 31 No. 2, pp. 357-381, doi: 10.1002/j.2158-1592.2010.tb00156.x.

Wang, Y., Wiegerinck, V., Krikke, H. and Zhang, H. (2013), "Understanding the purchase intention towards remanufactured product in closed-loop supply chains: an empirical study in China", *International Journal of Physical Distribution and Logistics Management*, Vol. 43 No. 10, pp. 866-888, doi: 10.1108/ijpdlm-01-2013-0011.

Wieland, A. and Wallenburg, C.M. (2013), "The influence of relational competencies on supply chain resilience: a relational view", *International Journal of Physical Distribution and Logistics Management*, Vol. 43 No. 4, pp. 300-320, doi: 10.1108/ijpdlm-08-2012-0243.

Windelberg, M. (2016), "Objectives for managing cyber supply chain risk", *International Journal of Critical Infrastructure Protection*, Vol. 12, pp. 4-11, doi: 10.1016/j.ijcip.2015.11.003.

Wirtz, B.W. and Weyerer, J.C. (2017), "Cyberterrorism and cyber attacks in the public sector: how public administration copes with digital threats", *International Journal of Public Administration*, Vol. 40 No. 13, pp. 1085-1100, doi: 10.1080/01900692.2016.1242614.

World Economic Forum (2023), *The Global Risks Report 2023, 17th Edition*, available at: https://www.weforum.org/publications/global-risks-report-2023/

Yang, L., Lau, L. and Gan, H. (2020), "Investors' perceptions of the cybersecurity risk management reporting framework", *International Journal of Accounting and Information Management*, Vol. 28 No. 1, pp. 167-183, doi: 10.1108/ijaim-02-2019-0022.

About the authors

Barbara Gaudenzi is Associate Professor in Supply Chain Management and Risk Management at the Department of Management at the University of Verona, Italy. She is Director of the master programs LogiMaster Plus and RiskMaster. Her research interests are, in particular, Supply Chain Management, Risk Management, and procurement strategies. Large part of her research has been published in international journals, such as Journal of Business Logistics, Industrial Marketing Management, International Journal of Production Economics, International Journal of Logistics Management, European Management Journal, Supply Chain Management: an international journal, and others. Barbara Gaudenzi is the corresponding author and can be contacted at: barbara.gaudenzi@univr.it

Benedetta Baldi is Ph.D. student in Accounting and Management – University of Verona and University of Udine. She works at the Department of Management at the University of Verona, Italy. Her research interests are, in particular, Consumer-centric supply chain management, Resilience, Sustainability, end-to-end supply chains, experimental methodology, and econometric modeling methods.