Computers & Security 137 (2024) 103591

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

The effect of environmental turbulence on cyber security risk management and organizational resilience

Susanne Durst [a,b,*], Christoph Hinteregger [c], Malgorzata Zieba [d]

[a] School of Business, University of Skövde, Sweden
[b] Department of Business Administration, Reykjavik University, Iceland
[c] Independent Researcher, Austria
[d] Department of Management, Faculty of Management & Economics, Gdansk University of Technology, Poland

ARTICLE INFO

Keywords:
Cyber security
Cyber security risk management
Resilience
Technological turbulence
Market turbulence

ABSTRACT

Even though there is a plethora of research on the role of environmental turbulence in organizational performance in general, little attention has been paid to the effect of environmental turbulence on cyber security risk management and further - organizational resilience. Drawing on the resource-based view and contingency theory, this study investigates how technological and market turbulence influence organizational cyber security risk management (CSRM) and then organizational resilience. Using a data set from 150 European companies, the study findings show how the two types of turbulence have different effects on CSRM in the companies studied. Technological turbulence directly impacts the firms' cyber security risk maturity while market turbulence has a direct positive affect on firms' cyber security risk perception. The study also determines the interplay between risk perception and risk maturity and subsequent resilience.

1. Introduction

Scholars frequently posit that the external environment influences the activities of organizations (Calantone et al., 2003; Siggelkow and Rivkin, 2005; Wilden and Gudergan, 2015). It is not surprising, therefore, that environmental turbulence is frequently the subject of research when investigating what direct or indirect influence it has on different firm activities, e.g., new product development (Calantone et al., 2003), product innovation performance (Puriwat and Hoonsopon, 2022), innovation quality (Luo et al., 2022), or product market diversification (Sun and Govind, 2017). External turbulence also increases the risks a company is exposed to (Wang et al., 2015; Foli et al., 2022). Risk management is assumed to be important to all types of organizations as it supports them in better handling both risks and opportunities (Oliveira et al., 2019). However, the degree of perceived importance that decision-makers attribute to risk management is likely to differ between organizations. Larger organizations are more likely than smaller organizations to have the necessary financial and non-financial resources for risk management (Crovini et al., 2021). Apart from the availability of resources, individual as well as socioeconomic factors also play a role (Etale et al., 2022).

The (business) world is exposed to technological turbulence, which in turn can trigger market turbulence, as customer preferences change (Jaworski and Kohli, 1993) due to the appearance of new products, market entrants and business models (Zhao et al., 2014; Jin et al., 2022). Turbulence related to new technologies also increase the danger of cyber risks/cyber-attacks (De la Peña Zarzuelo, 2021; Lee, 2021), thus making companies more vulnerable (Radanliev et al., 2020). Therefore, one would expect that companies react and adjust their cyber security risk management (CSRM) as part of their overall enterprise risk management (ERM) accordingly, and hence, step by step they become more mature (Dellana et al., 2022). Companies that are more mature from a (cyber risk) management point of view are also expected to be more resilient (Colicchia et al., 2019; El Baz and Ruel, 2021) and further, resilient organizations are better prepared for dealing with environmental turbulence (Burnard and Bhamra, 2011; Jiang et al., 2019).

There is a paucity of research that has empirically examined the direct effects of environmental turbulence on risk management, particularly with regard to cyber security risks. Therefore, the purpose of this paper is to examine how environmental turbulence (i.e., market turbulence and technological turbulence) affects the relevance of cyber security risk management and thus, the resilience of organizations. With the ever-increasing need to assess different types of risks, improving the resilience of organizations appears pressing (Sawalha, 2015; Andersson

* Corresponding author.
E-mail address: susanned@ru.is (S. Durst).

https://doi.org/10.1016/j.cose.2023.103591
Received 9 July 2023; Received in revised form 7 October 2023; Accepted 6 November 2023
Available online 10 November 2023

et al., 2019). In particular, the following research questions are formulated and need to be answered: What is the effect of different types of environmental turbulence on the importance of cyber security risk management in organizations? What is the effect of cyber security risk management on organizational resilience? The research draws on the resource-based view (RBV) and contingency theory. The former is assumed to help organizations set priorities in (CS)RM, while the latter helps understand company behavior in the context of environmental turbulence.

The paper contributes to the state of the art in the following way. The study deepens the understanding of the role of different types of environmental turbulence on the preparedness of organizations to invest more in CSRM to enhance organizational resilience. The findings can also facilitate the development of more resilient organizations.

The paper is organized as follows. Next, the relevant literature and its constructs are presented, it also includes the development of hypotheses. Then, the method is outlined, and the results are analysed. Finally, the study's contributions, its implications, limitations, and avenues for future research are presented.

2. Theoretical background and related work

Research in the field of risk management has increased significantly in recent years (Gordon et al., 2009; Gates et al., 2012; Aebi et al., 2012; Hoffmann et al., 2013; Durst et al., 2019; Munir et al., 2020), the same appears to apply to the study of CSRM or related areas (Lee, 2021; Gatzert and Schubert, 2022; Shaikh and Siponen, 2023). In particular, the pandemic and the war in Ukraine seem to have given further impetus to CSRM research (Kure et al., 2022; Georgiadou et al., 2022).

2.1. Cyber security and cyber security risk management

Cybersecurity refers to the preservation of the confidentiality, integrity, and availability of information in complex environments resulting from the interaction of people, software, and services on the Internet using technology devices and connected networks (ISO/IEC, 2012). Cybersecurity has become an important issue for all businesses as more and more devices are interconnected, which in turn has significantly increased the potential for cyberattacks (Lee, 2021). A lack of active measures in this area not only opens up the possibility for cybercriminals to access sensitive data, but also to paralyze the entire information systems (IT) infrastructure of organizations (Miller et al., 2021; Chowdhury and Gkioulos, 2021). Hence, CSRM has been defined as "the process of identifying, analyzing, and addressing an organization's IT security risks to prevent future cyberattacks and account for ongoing cyberthreats" (https://www.eccouncil.org/cybersecurity-exchange/executive-management/effective-cybersecurity-risk-management-checklist/). Scientific research in this area from a management perspective seems still in its infancy and targeted activities are predominantly found in practice. These activities are, unsurprisingly, strongly driven by management consultancies in general or IT-focused consultancies, as well as other companies dealing with data security, etc.

When the practice of CSRM is considered, recently Coden et al. (2023) have reported that even though many organizations evaluate their cyber maturity (CM), there seems to be an imbalance in the focus. Efforts and investments seem to be mainly focused on the first phases of risk management, i.e., identification, protection, and detection. Response, recovery, and business continuity receive less attention and support. Considering the number of attacks that have been reported recently – the Flash Eurobarometer 496 SMEs and cybercrime of the European Union (2022) reported that 28 % of European SMEs have experienced at least one type of cybercrime in 2021 - and also the costs of these cyber incidents – Statista (2023) stated that the global average cost of a data breach between March 2021 – March 2022 was 4.35 million U.S. dollars – this focus of the companies is surprising and suggests that companies are poorly prepared for any damage repair. Even more worryingly, a recent study by the German insurance company HDI published in April 2023 indicated that the issue of cyber security has fallen out of focus for many German companies compared to the results of the last study (https://www.versicherungsbote.de/id/4910502/KMU-Wahrnehmung-von-Cyberrisiken-sinkt/).

2.2. Cyber security risk management and resilience

A company's decision to invest in CSRM and its continuous improvement is also likely to contribute to the company's resilience (Aven, 2019). The origin of concept of resilience in the management field can be tracked back to the 1980s, when two seminal papers were published by Staw et al. (1981) and Meyer (1982). Both papers discussed variation–selection–retention mechanisms and proposed different ways how organizations may respond to external threats (Linnenluecke, 2017). Since the publication of these papers, resilience in literature has been examined and perceived in a variety of ways. For example, Ovans (2015) defines organizational resilience as "the ability to recover from setbacks, adapt well to change, and keep going in the face of adversity" (p.1). According to Dahles and Susilowati (2015), resilience is related to the capacity of an enterprise to "survive, adapt, and grow in the face of turbulent change" (p. 37), while in the opinion of Radović (2018), it means "the ability of an organization to rapidly adapt and respond to internal or external changes and continue operations (…) and it also directly contributes to faster and more successful recovery of the community after the crisis or disaster" (p. 5). All in all, it can be concluded that organizational resilience is related to the ability of an organization to handle changes and turbulences, both internally and externally in a way that allows it to continue its operations and adapt.

2.3. Turbulence

Organizations are part of an external environment that has become more dynamic and uncertain over time. Turbulent environments are characterized by changing customer preferences, frequent technological changes, and more intense competition (Droge et al., 2008). In the context of new product development (NPD), Calantone et al. (2003) described a turbulent environment as "one in which frequent and unpredictable market and/or technological changes within an industry accentuate risk and uncertainty in the NPD strategic planning process" (p. 91). As a result, a turbulent environment contributes to companies' awareness of the need to be innovative and proactive (Siggelkow and Rivkin, 2005; Madrid-Guijarro et al., 2009; Tsai and Yang, 2014). In this paper, it is argued that the inclusion of turbulence is useful for enriching the understanding of organizational efforts regarding CSRM and hence organizational resilience.

2.4. The theoretical underpinnings: contingency theory and resource-based view

The paper is based on two theories, namely contingency theory and the resource-based view approach.

The contingency theory of organizational structure provides one of the most important frameworks for the study of organizational design. It claims that the most effective organizational structural design is based on the structure suiting the contingencies (Burton et al., 2006). In other words, contingency theory argues that business performance depends on the relationship or fit between an organization and its internal and external environment. Thus, the theory helps to understand how organizations align their expected performance with the environment, while emphasizing the external environment (Pratano, 2016). The contingent factors include technology and culture, which are expected to influence the design and function of organizations. Contingency theory assumes that there is no single type of organizational structure that could fit equally in all organizations, but rather, organizational effectiveness depends on a match between the kind of technology, environmental

unpredictability, the size of the organization, the characteristics of organizational structure and the applied information system (Islam, 2012). The contingency perspective has been shown to be appropriate in studies that address relationships between environment, strategy, organizational structure and performance (Calantone et al., 2003). According to Luthans and Stewart (1977), the contingency theory is based on "identifying and developing functional relationships between environmental, management and performance variables" (p.183). Therefore, for the purpose of the present study, the contingency theory offers the possibility to include several elements in the analysis of the fit between the organization and its contingencies. Organizational resilience could potentially depend on such contingent factors as environmental turbulence or CSRM.

The resource-based view (RBV), on the other hand, postulates that resources play the key role in creating and sustaining organizational competitive advantage. According to Barney (1991), resources are "all assets, capabilities, organizational processes, firm attributes, information, knowledge, etc., controlled by a firm that enable the firm to conceive of and implement strategies that improve its efficiency and effectiveness" (p.101). For these resources to be useful and successful in offering sustained competitive advantage, they must follow the so-called VRIO characteristics, namely, they need to be valuable (they exploit opportunities or eliminate threats from the environment); rare among the present and potential competitors; imperfectly imitable; exploitable by the firm's organization (Barney, 2001). The RBV further assumes the heterogeneity of the resources in the sense that resources vary across organizations and can become a source of competitive advantage (Alvarez and Busenitz, 2001). Considering the aim of this study and the RBV as an additional theoretical underpinning, it can be assumed that CSRM might be perceived as one of the intangible resources an organization possesses, which can be unique and difficult to imitate and contribute not only to a better position on the market, but also to increased resilience. It is based on the assumption that some organizations are better at CSRM than others and this can contribute to a stronger resilience. These more successful organizations are assumed not only to be aware of their finite resources, but also to use them according to their relevance for the benefit of the organization.

2.5. Related work

After presenting the relevant concepts and perspectives of the work, the following section focuses on studies that have studied CSRM to highlight the contributions of this study to advancing the field. Henri (2013) utilized an exploratory case study approach to identify and discuss Supervisory Control and Data Acquisition (SCADA) systems cyber security challenges. Data were collected by the means of individual interviews, workshops, and breakout focus group meetings involving stakeholders of oil and gas critical infrastructure SCADA system cyber security programmes. The findings stress the relevance of a risk-based assessment methods for engineering managers and decision makers to bring them in a better position to allocate their efforts to those areas where the highest return on investment can be expected. Meszaros and Buchalcevova (2017) developed and proposed a framework for online services security risk management. It was based on the Design Science Research methodology and verified through a case study that was performed in one large organization that acts both as an online service provider and consumer. Alahmari and Duncan (2020) did a systematic literature review, including 15 papers, on CSRM in small and medium-sized enterprises (SMEs). The authors found that current research has primarily been conducted in developed countries and emphasised five perspectives namely cyber security threats, behavior, practice, awareness, and decision-making. Based on the results the authors conclude that informed cyber security decision-making relies on the perspectives threat, behavior and awareness to identify and apply the right procedures. By also focusing on SMEs, Benz and Chatterjee (2020) developed a methodology that can inform SME IT leaders about their cybersecurity risk exposure and based on that provide strategies for risk reduction. The authors collected feedback on the methodology from 12 individuals. Ganin et al. (2020) developed a risk-based decision framework for cybersecurity strategy prioritization that includes the TVC (threats, vulnerabilities and consequences) components of risk and uses an illustrative example to show how the proposed framework could be used for risk mitigation. Lee (2021) proposes a cyber risk management framework consisting of four layers which are the cyber ecosystem layer, the cyber infrastructure layer, the cyber risk assessment layer, and the cyber performance layer. The framework is illustrated based on real-world scenario; the discussion has a focus on IT projects. Hoppe et al. (2021) used market insights from 37 industry surveys to learn about the current state of SMEs' cyber risk management process. Based on their review, the authors stress the need for more research on the influence of cyber security culture (i.e., cyber risk competency, cyber risk awareness and managerial attitudes) on SMEs' vulnerability and on the maturity of the risk management process. Eling et al. (2021) did a review on research on the different steps of the cyber risk management process. Among other things, the authors identify a research gap regarding the potential link between cyber risk management and resilience. They also established a shortage of studies providing empirical evidence on cyber security research other than the United States.

In summary, it can be said that the existing scientific research in the field of CSRM in general and with regard to a management perspective in particular is still in its infancy. The number of papers that empirically investigate CSRM in businesses is small and conceptual or theoretical papers predominate to date. This situation is addressed in this study by presenting empirically insight into the link between CSRM and organizational resilience. The effects of turbulence to this equation allow an even better understanding of this link. Primary data is provided from European organizations of different size.

3. Research model and hypotheses development

In this study, the link between turbulence and CSRM and eventually organizational resilience is examined. The research model is depicted in Fig. 1 and the related hypotheses are presented in the following sections.

3.1. Cyber security risk management

In this study, two constructs of CSRM are included that are directly related to (cyber security) risk management. First, risk perception (RP) which has been defined as "the subjective assessment of the probability of a specified type of accident happening and how concerned we are with the consequences" (Sjöberg et al., 2004, p. 8). RP goes beyond the individual, but is a social and cultural construct reflecting values, symbols, history, and ideology (Weinstein, 1989). Existing literature has shown that risk perception largely influences risk management (Bubeck et al., 2012; Marshall, 2020). Therefore, the authors of this paper assume the same link for CSRM and expect that high levels of risk perception among decision-makers enhance their preparedness to prioritize CSRM as an important business function for organizational resilience. Second, the level of RP contributes to organizations' evolutionary progression regarding CSRM, thus their level of maturity (Proença et al., 2017). Therefore, the following hypothesis is postulated:

- H1: Cyber security risk perception positively influences cyber security risk maturity.

There is empirical evidence that the maturity level has an impact on organizational performance (Hartono et al., 2014; Farrell and Gallagher, 2019). In a more recent study, Hartono et al. (2019) have demonstrated how contextual variables such as complexity (in their study project complexity) can moderate the relationship between risk management maturity and performance, which, in turn, means that "the more, the better" is not the automatic consequence. Possible reasons for

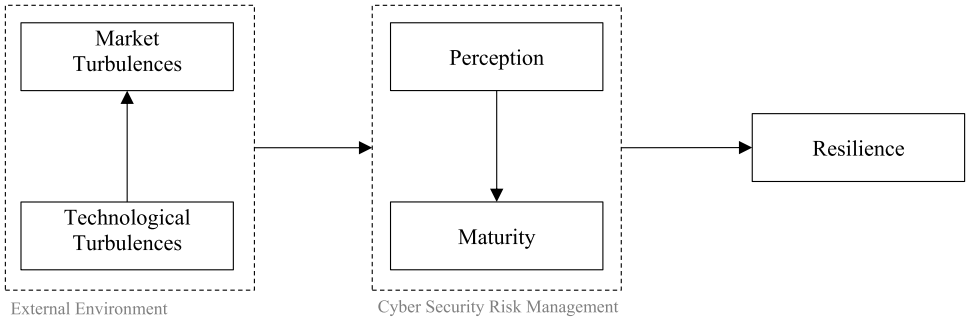


Fig. 1. The Research Model of the Study.

a company's continuous improvement of CSRM are its contribution to business performance and risk mitigation in uncertain environments (Committee of Sponsoring Organizations of the Treadway Commission, 2017). In summary, decision-makers have a strong responsibility to promote active engagement of the workforce to create an environment that is interested in the continuous development of RM in general and thus, actively contribute to the well-being of the whole company.

3.2. Cyber security risk management and resilience

As far as resilience in the context of risk management is concerned, recent work in this area suggests that risk management is critical for resilience (Settembre-Blundo et al., 2021; Singh, 2022); it forms its entry point (Mitchell and Harris, 2012). At the same time, risk management requires amendments to be better prepared for emergent forms of risks (Smith and Fischbacher, 2009). Risk management in organizations must become holistic and more dynamic (Fehle and Tsyplakov, 2005; Mikes, 2009). The same can be expected for CSRM. Since risk management is not only a demanding business function, but also a costly one (Callahan and Soileau, 2017), it can be argued that more mature organizations will benefit more from CSRM in terms of its contribution to resilience.

Hence, the following hypothesis is posed:

- H2: Cyber security risk maturity positively influences resilience.

3.3. Technological turbulence and market turbulence and cyber security risk management

This study considers technological turbulence and market turbulence. Song et al. (2005) defined technological turbulence as the rate of change and unpredictability of technology in an industrial or market environment. Such an environment favours shorter product and product development cycles (Tsai and Yang, 2014). However, technological turbulence does not only increase the number of new business opportunities (Bodlaj and Čater, 2019), but also the number of risks (Temel and Durst, 2021).

Market turbulence, which has been defined as the rate of changes in customer preferences (Jaworski and Kohli 1993), affects companies' conduct and thus, their organizational performance (Bodlaj and Čater, 2019). The market is constantly breaking and reshaping traditional boundaries of industries (Qiu et al., 2020), i.e., customer preferences, price/cost structures and the competition of competitors change continuously (Cantalone et al., 2003). Based on contingency theory, it could therefore be concluded that market turbulence also influences the strength of a firm's response. Consequently, firms operating in markets with unstable customer preferences are forced to adapt their offerings to the changing needs of customers (Jaworski and Kohli 1993). Firms that are not only highly adaptable to ever-changing markets, but are also highly innovative, may be able to develop new processes that improve their understanding of the markets they serve. Based on the above discussion, it is assumed that technological turbulence in particular contributes to market changes (market turbulence) (Christensen, 1993; Wang et al., 2013) and therefore, the following hypothesis is formulated:

- H3: Technological turbulence positively influences market turbulence.

To address the risks inherent in environmental turbulence, organizations must assure that their CSRM is up to date so that organizational resilience is not negatively affected. Consequently, a stronger (even a first-time) emphasis on risk management is assumed. The consequences of the pandemic (Ferguson and Drake, 2021) and the invasion of Ukraine (Korosteleva, 2022) clearly indicate this assumption. Therefore, in a turbulent environment, it is expected that there will be a greater focus on CSRM to reduce the organization's vulnerability in general and to the increasing number of cyber threats and attacks in particular (Gaurav et al., 2022). As a result of these two events, as well as others such as advancing climate change, the environment has become even more turbulent. Overall, it can therefore be expected that decision-makers will not only react more quickly to technological and market turbulence, but also increasingly promote the development of CSRMs in order to better capture the associated even further increased uncertainty. It is therefore argued that not only has risk perception increased, but that the turbulence has also encouraged the organizations to move towards higher risk maturity. In addition to individual factors, e.g., personal risk perception and risk experience (Barnett and Breakwell, 2001), contextual factors influence decision-makers' willingness to accept different levels of risks (Calantone et al., 2003). It means that risk takers are more comfortable with making decisions in turbulent environments than risk avoiders.

Based on these considerations, the following hypotheses are formulated:

- H4: Technological turbulence positively influences cyber security risk perception.
- H4a: Market turbulence positively influences cyber security risk perception.
- H5: Technological turbulence positively influences cyber security risk maturity.
- H5a: Market turbulence positively influences cyber security risk maturity.

Based on the above, the following research model is proposed (Fig. 1).

In the following sections, the methods used in the research will be presented and the hypotheses will be tested.

4. Method

4.1. Sample and data collection

The study was conducted in November 2021 with the support of the Prolific tool, which allowed the distribution and selection of online

questionnaires among the defined sample of respondents. The questionnaire was entitled "Knowledge Risks in Organizations" and had the description of "In this study you will be asked about knowledge risk management in your organization (e.g., about cyber risks)". This title and the description clearly indicated what is the subject of the study and was the first signal to the respondents to determine if they were eligible to participate in this study. The questionnaires were sent out to potential candidates meeting all of the following requirements: the minimum age of 25 years old, fluent in English, with one of the following roles: Upper Management, Middle Management, Junior Management, Self-employed/Partner, and with one of the following highest levels of education completed: Technical/community college, Undergraduate degree (BA/BSc/other), Graduate degree (MA/MSc/MPhil/other), Doctorate degree (PhD/other) and originating from one of the following countries: Germany, France, Spain, Italy, or Sweden.

Convenience sampling was used to send the questionnaire to participants fulfilling the requirements from the countries such as Germany, France, Spain, Italy, and Sweden. Due to growing problems in accessing study participants and convincing them to take part in the study, convenience sampling is a common, efficient and useful technique to collect a general overview of the phenomenon of interest (Chong et al., 2011; Leiner, 2017). Managers and partners were contacted by the use of company lists. In total, 182 responses were collected. To ensure the quality of the data, only fully completed questionnaires entered the analytical stage, which resulted in a final set of 150 questionnaires. These responses constitute a European sample dominated by responses from Germany, Italy, and Spain (22.0 % each).

The sample includes firms with various ownership profiles such as family (22 %) and non-family businesses (42 %), firms that are part of a corporate group (30.7 %) as well as public firms (3.3 %). 40 % of the firms in the sample are large firms employing more than 250 people. 60 % are small- and medium-sized enterprises (SMEs). The average age of the firms in this study is 35 years with a standard deviation of 53 years. The firms are distributed over 12 different sectors, whereas information and communication technology sector (ICT) counts up for 20.7 % of the firms, followed by the manufacturing (13.3 %) and professional, scientific and technical sector (12.0 %).

Table 1 shows the sample characteristics regarding firm size, firm type, and firm location.

4.2. Measures

The major constructs in this study include market and technological turbulence, cyber security risk perception and maturity, as well as resilience.

For measuring both types of turbulence, items proposed by Jaworski and Kohli (1993) were used which continue to be topical and which were used in similar studies (e.g., Bodlaj and Čater, 2019; Foli et al., 2022).

Table 1
Sample Characteristics.

Characteristic	*Dimension*	*No*	*%*
Firm size	Micro (< 10 employees)	31	20.7
	Small (< 50)	35	23.3
	Medium (< 250)	24	16.0
	Large	60	40.0
Firm type	Family-business	33	22.0
	Non-family-business	63	42.0
	Part of a corporate group	46	30.7
	Other	8	5.3
Firm location	France	15	10.0
	Germany	33	22.0
	Italy	32	21.3
	Spain	32	21.3
	Sweden	5	3.3
	Other	33	22.0

Note: $n = 150$.

Market turbulence describes the rate of change in the composition of customers and their preferences. Consequently, organizations that operate in highly turbulent market environments, must update their products and services continuously in order to satisfy customer needs (Jaworski and Kohli, 1993), which may expose organizations to cyber security risks at a greater extend. The level of market turbulence was calculated as the average score of the following items using a 7-ponit Likert scale ranging from "Strongly disagree" to "Strongly agree": In our kind of business, customers' product/service preferences change quite a bit over time; Our customers tend to look for new products/services all the time; Sometimes our customers are very price-sensitive, but on other occasions, the price is relatively unimportant; We are witnessing demand for our services from customers who never bought them before; and new customers tend to have service-related needs that are different from those of our existing customers.

Technological turbulence describes the rate of technological change. Organizations that make use of nascent technologies may be able to gain a competitive advantage through technological innovation (Jaworski and Kohli, 1993), while at the same time are more exposed to technological risks in terms of cyber security risks. The level of technological turbulence was calculated as the average score of the following items using a 7-point Likert scale ranging from "Strongly disagree" to "Strongly agree": The technology in our industry is changing rapidly; Technological changes provide big opportunities in our industry; It is difficult to forecast where the technology in our industry will be in the next 2 to 3 years; A large number of new product ideas have been made possible through technological breakthroughs in our industry; and Technological developments in our industry are rather minor.

To measure cyber security risk perception, cyber risk maturity, and resilience, this study utilised items derived from the Global Cyber Risk Perception Survey (Marsh and McLennan Companies, 2018). Consequently, to measure cyber security risk perception, respondents were asked to rate their organizations perception regarding the importance of cyber security risks for their organization on a 5-point Likert scale ranging from not important to most important.

According to The Global Cyber Risk Perception Survey (Marsh and McLennan Companies, 2018), cyber risk management requires a comprehensive approach to address the accelerating complexity. Hence, organizations are forced to focus on the entire life cycle including risk assessment, mitigation, and responsiveness. Following this line, cyber security risk maturity was calculated as an average score out of three items measured on a 5-point Likert scale ranging from "Not at all confident" to "Highly confident". Respondents were asked to rate the organization's level of confidence regarding cyber risk security identification and assessment; mitigation and prevention; and their responsiveness and recovering ability compared to their key competitors.

To measure resilience, this study adopted items from previous research on risk management (Durst et al., 2019). Hence, resilience was calculated as the average score of four items. More specifically, respondents were asked to rate their respective organization's performance in terms of innovation, sustainability, agility and better responsiveness compared to their main competitors. This was done using a 7-point Likert scale (ranging from "Strongly disagree" to "Strongly agree").

Finally, following previous research on organizational resilience, this study controlled for firm characteristics that could influence the relationship between cyber security risks and resilience in organizations. As larger firms can use resources, capabilities and processes to enhance risk identification and mitigation, these firms tend to be more resilient to changes in the external environment (El Baz and Ruel, 2021). Consequently, firm size (in terms of the number of employees) was included in the model. Additionally, the study controlled for the age of an organization as it may influence an organization's attitude to risk management

and thus the organization's level of maturity regarding CSRM (c.f. Hoffmann et al., 2013). Therefore, this study incorporated age (in terms the number of years since its foundation) as a second control variable.

This study utilised subjective self-report measures to measure the major constructs in this study. Although the questionnaire consisted of several response options (yes/no answers, different Likert scales, etc.), a concern with self-construction questionnaires arises from the common method variance (CMV). Therefore, we executed the Harman's single-factor test including all variables of the study (Love et al., 2014). CMV is an issue, if the single factor calculated accounts for the majority of the covariance among the measures (Podsakoff et al., 2003). However, as the calculated factor accounts for 31.72 % of the variance only - and thus for less than the majority - CMV did not seem to be a problem in this study.

Additionally, a pre-test was executed with three persons from the upper management fulfilling the requirements to further moderate the weaknesses of self-administered surveys (Saunders et al., 2007). Finally, past research has shown some clear evidence that the criticism of self-report measures is unjustified (Richard et al., 2009). Wall et al. (2004), for example, has found a correlation of 0.6 between objective and subjective measures, a high level of discriminant validity, whereas Guthrie (2001) found correlations up to 0.81.

4.3. Statistical method

To test the hypothesized relationship between market and technological turbulence, cyber security risk perception and maturity, and resilience, a structural equation modeling (SEM) approach was applied using the AMOS software, version 23. SEM is viewed as an appropriate technique to study multiple correlated independent and dependent variables (e.g., Wei et al., 2008; Lundqvist, 2015; Sturm et al., 2022). Due to the correlation of the independent variables, in conventional methods such as multiple regressions, some of the independent variables needed to be controlled in order to generate a unique variance (Wei et al., 2008). By contrast, SEM allows the integration multiple correlated independent variables as well as latent variables and offers the ability to account for measurement errors within the estimation process (Hair et al., 1998).

To evaluate model fitness, we followed the suggestion of Hu and Bentler (1999) and used a multi-index presentation format including:

- the standardized root mean squared residual (SRMR), which analyses the discrepancies between the observed correlation and the correlation matrix implied by the model (Kline, 2010). Hu and Bentler (1999) suggest a SRMS below 0.08 to indicate a good fit of the model.
- the Tucker-Lewis Index (TLI), also known as the non-normed fit index, which analyses the discrepancy between the hypothesized and null model by evaluating a very specialized covariance structure to correct the drawback of the normed fit index for smaller sample sizes (Bentler and Bonnet, 1980). According to Hu and Bentler (1999) good model fitness is present, if TLI is above 0.95.
- the comparative fit index (CFI), which analyses the discrepancy between the data and the hypothesized model (Gatignon, 2010). Hu and Bentler (1999) suggest a CFI above 0.95 to indicate good model fitness.
- and the root mean square error of approximation (RMSEA), which analyses the mean absolute correlation residual to provide information about the "badness of fit" (Kline, 2010). Consequently, Hu and Bentler (1999) suggest a value below.06 to indicate good model fitness.
- the Chi-Square statistics are reported as well, although previous research reported a lack of power for smaller samples (Kenny and McCoach, 2003).

5. Results

Table 2 reports the means, standard deviations, and correlations among the major study variables.

Not surprisingly, firm size and firm age are highly correlated with each other ($r = 0.575$, $p < .01$). Additionally, firm size is highly correlated with cyber security risk perception ($r = 0.324$, $p < .01$) and a firm's cyber security risk maturity ($r = 0.314$, $p < 0.01$).

Turning to our variables of interest, Table 2 reports a significant positive correlation among all major study variables, except the relationship between cyber security risk perception and resilience ($r = 0.135$, $p > .05$).

The path diagram in Fig. 2 illustrates the entire structural model.

Results show that SRMR (< 0.08), RMSEA (< 0.06), CFI (> 0.95), and TLI (>= 0.95) report a good model fit and therefore we conclude that our structural model provides a good fit for our data. Despite the limitations of the Chi-square test for smaller samples, the test results show a good fit for our data as well. Regarding the dependent variables, results show a significant direct effect of the firm's cyber security risk perception on its cyber security risk maturity ($r = 0.32$, $p < .01$) which in turn positively influences the resilience of the firm ($r = 0.32$, $p < .01$). Hence, results fully support hypotheses H1 and H2.

Additionally, we proposed that the firm's market environment in general and its technological environment in particular are highly interconnected. More precisely, we stated that technological turbulence has a positive impact on market turbulence (H3) which in turn influences a firm's cyber security risk management. Results confirm that the more volatile a firm's technological environment is, the more turbulences in the general market environment of the organization exists ($r = 0.52$, $p < .01$).

Hypotheses 4 and 5 stated that technological and market turbulences influence a firm's cyber security risk management. However, results show only mixed support for these hypotheses. While technological turbulences only directly impact the firm's cyber security risk maturity ($r = 0.20$, $p < .05$), market turbulences only have a direct positive effect on the firm's cyber security risk perception ($r = 0.23$, $p < 0.05$). Hence, only support for hypotheses H4a and H5 was found, while hypotheses H4 and H5a were rejected.

The results of the tests are summarized in Table 3.

6. Discussion and conclusion

This study has adopted contingency theory and RBV of the firm, using a sample of 150 organizations, to empirically analyze the effects of environmental turbulence on CSRM, i.e., CSR perception and CSR maturity. The results confirm that cyber security risk perception positively influences cyber security risk maturity (H1). It suggests that a crucial first step in implementing CSRM is to be aware of the potential cyber risks to which the organization may be exposed and their possible consequences, and then to act in the next step, in terms of a continuous investment in the organization's CSRM (i.e., CSRM maturity). This is consistent with the findings of Alahmari and Duncan (2020) regarding the importance of awareness (perception) in CSRM.

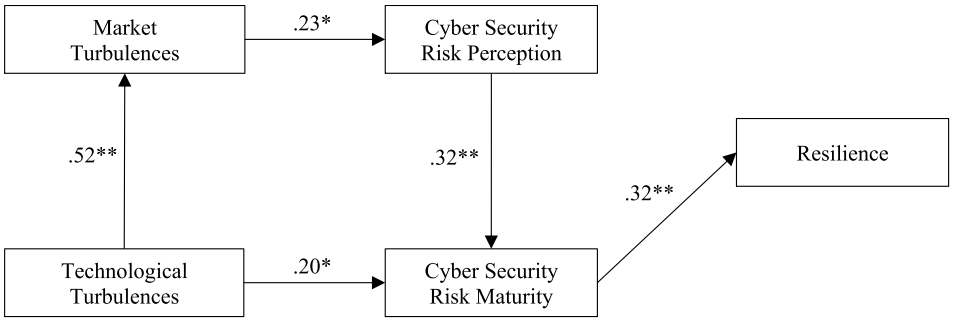
The results also show that environmental turbulence has a significant and positive impact on both CSR perception and SCR maturity and then enhance organizational resilience. The higher the CSR perception, the more decision-makers will place CSR maturity in the core to strengthen organizational resilience (H2). Moreover, the study confirms the driving force of technological turbulence on market turbulence (H3). This demonstrates the power of new technologies or technological solutions on markets and their structure and offerings and is in line with previous studies (Christensen, 1993; Wang et al., 2013).

The study confirms the role that environmental turbulence plays in driving organizations' CSRM efforts. Both market and technological turbulence increase CSRM, however, their influence varies. Market turbulence positively influences CSR perception (H4a) while

Table 2
Means, Standard Deviations, and Correlations among Variables.

Variable	*Mean*	*S.D.*	*1*	*2*	*3*	*4*	*5*	*6*	*7*
1. Firm age [a]	3.05	0.98	1.00						
2. Firm size	2.76	1.18	.575**	1.00					
3. Technological turbulence	3.17	0.52	.051	.143	1.00				
4. Market turbulence	3.07	0.59	.057	.108	.449**	1.00			
5. Cyber security risk perception	2.37	0.91	.124	.324**	.151	.230**	1.00		
6. Cyber security risk maturity	2.06	0.66	.122	.314**	.296**	.206*	.410**	1.00	
7. Resilience	3.31	0.68	.012	.066	.280**	.207*	.135	.320**	1.00

Note: $n = 150$; correlation coefficient is significant at * $p < .05$ (two-tailed), ** $p < .01$ (two-tailed).
[a] Firm age is calculated by the natural log of years since firm foundation.



Notes: n = 150; standardized coefficients significant at ** p < 0.01, * p < 0.05
Controls: firm size, firm age
Model fit: χ^2 = 18,776, *df* = 13, SRMR = .078; RMSEA = .055, CFI = .969, TLI = .950

Fig. 2. Structural Model of Cyber Security Risk Perception and Maturity, and Resilience
Notes: $n = 150$; standardized coefficients significant at ** $p < .01$, * $p < .05$
Controls: firm size, firm age
Model fit: $\chi^2 = 18{,}776$, $df = 13$, SRMR = 0.078; RMSEA = 0.055, CFI = 0.969, TLI = 0.950.

Table 3
Results of hypotheses testing.

Hypothesis	*Result*
H1: Cyber security risk perception positively influences cyber security risk maturity	✔
H2: Cyber security risk maturity positively influences resilience	✔
H3: Technological turbulence positively influences market turbulence	✔
H4: Technological turbulence positively influences cyber security risk perception	×
H4a: Market turbulence positively influences cyber security risk perception	✔
H5: Technological turbulence positively influences cyber security risk maturity	✔
H5a: Market turbulence positively influences cyber security risk maturity	×

Note: ✔ = confirmed; × = rejected.

technological turbulence positively influences CSR maturity (H5). A possible explanation for the difference may lie in several factors. First, in case of market turbulence, such a kind of changing environment related to customers and their needs requires from the organization the constant scanning of the market and, at this occasion, the organization might also come across the cyber security risks emerging from this market. In this case, the organization is likely to increase its perception of those cyber security risks and become also knowledgeable about their possible consequences. However, an organization's ability to deal with these risks will not automatically increase as well. Past research has shown the difficulties in achieving this link (e.g., Silva et al., 2013; Tsohou et al., 2015). In fact, perception is only the beginning. Organizations need to have social relationships, culture and traditions to move from perception to concrete successful actions/results (c.f., Wilkins, 1989) and this in turn seems to support cyber security maturity. Secondly, in the case of technological turbulence, the organization might be forced to carefully evaluate not only the changing technologies and new solutions, but also the ways they are applied in the organization; and also very likely, what needs to be changed in the organization to adopt the new technological solutions successfully (Edirisinghe and Pinsker, 2020). In this way, the organization could become more mature regarding CSRM, as it not only acquires new theoretical knowledge about new technologies and their consequences but can also use it for its own benefit (security). The organization is therefore also developing the knowledge of how to protect the company from cyber risks that may arise from the use of new technologies. A very simple example relates to new computer equipment and software. When the organization purchases such equipment, it normally also purchases the means of protecting it against cyber risks, i.e., anti-virus software and a variety of means to minimize the risk of cyber-attacks. This way, the organization not only applies new technology, but also increases its ability to better cope with possible cyber risks. In other words, the use of new technology brings with it the risk of cyber-attacks and other cyber risks, which in turn means that the organization's CSRM needs to be updated; these activities in turn contribute to increased CSR maturity. The greater the technological turbulence and the need to update and implement new technologies (technology push), the more mature the organization might become with regard to CSRM. Environmental turbulence would thus act as direct antecedent to the continued investment in CSRM and thus organizational resilience.

6.1. Theoretical and practical implications

This study makes several contributions to the literature. First, to the best knowledge of the authors, this is the first study examining cyber security risk management in the context of market and technological turbulences and linking those concepts to organizational resilience. Until now, those phenomena and their interrelations have not been examined in organizations. Thus, this paper makes a valuable contribution to advancing research on cyber security (risk) management in general and the relationship between CSRM and resilience in particular (Eling et al., 2021).

Second, the study's findings underline that CSRM provides value to organizations. Thus, this study contributes to research about the value relevance of risk management (Viscelli et al., 2016; Willumsen et al., 2019). This is especially important taking into account that CSRM is often very costly for organizations and hence they might restrain from investing in it without knowing the potential outcome and benefits for themselves. Our paper proves that this kind of investment might indeed bring measurable benefits to organizations, in the form of increased resilience, and, as such, it contributes to the theory and practice in this area (Settembre-Blundo et al., 2021; Singh, 2022), but also to the research direction that is interested in the antecedents of resilience (Rodríguez-Sánchez et al., 2021; Eling et al., 2021).

Considering the influence of CSRM on organizational resilience, decision-makers should work hard to make risk management in general a top priority and permanently communicate its importance to all organization members. This aspect is crucial, as cyber risks can appear at all organizational levels and therefore, only by integrating CSRM at all organizational areas and levels, organizations might count on better results and benefits. The link between CSRM and organizational resilience should be strongly emphasised, also to justify the importance of investing not only in financial, but also human and organizational resources regarding CSRM. Working steadily on CSRM enables organizations to achieve better organizational resilience and help them overcome the negative consequences of turbulences. Hence, all types of organizations are advised to invest financial and non-financial resources and time in improving their CSRM step by step. However, it should not be forgotten that higher commitment does not automatically lead to greater success (Durst et al., 2019).

As market turbulence increases CSR perception, organizations are advised to closely monitor changes in their respective markets to quickly recognize and evaluate new opportunities and challenges. Similarly, as technological turbulence impacts CSR maturity, organizations should also closely monitor these developments and assess possible implications of them on the organization's business operations and models. Against this background, continuous training of all staff in (CS)RM as well as market research should be of utmost importance. The results presented in this study also underline the importance of the underlying idea of ERM for organizations, a holistic approach is required to better assess and then, if necessary, solve the problems mentioned above.

6.2. Limitations and future research

The main limitation of the present study is that it examined a limited number of components of CSRM. Future research could consider other relevant components of CSRM, such as risk governance, risk assessment, and responses. Adding those components as well as other could further strengthen the explanatory power of the proposed model. Another limitation is that the results are based on a cross-sectional study.

Due to the use of convenience sampling technique, the generalizability of the study is somewhat limited and hence, future research could investigate the relationship under investigation in different populations or using random sampling techniques to enhance the generalizability of the findings. Another limitation arises with the construction of the questionnaire. In this study, cyber security risk perception is measured using a single-item and hence might not capture the construct of cyber risk perception in its entirety. Therefore, futures studies could rely on more sophisticated measures to address cyber security risk perception in a more comprehensive manner. The sample included in this study did not allow to run an analysis that included cultural or industry-specific factors. This is another potential future research area.

Changes in risk management over time could not be captured but would be important to understand as turbulence and risk are both dynamic concepts and therefore require constant attention. Even though the focus of this paper is mainly on cyber risks, this does not mean that a silo perspective on risk management should be followed (or continued), quite the contrary. In line with ERM, a holistic and strategic view of risk management in organizations should be applied to address all types of risks, as well as opportunities. Thus, contemporary risk management should be based on coordinated and integrated actions that are focussed on all kind of risks and underlines that ERM should be handled at the top leadership and not be simply delegated to other departments, e.g., the IT department.

Future research could explore how risk management in companies can be permanently adapted and practiced not only to cover new, previously unknown risks, but also to prevent certain risks from attracting more attention than they deserve. Some risks might be more important for some organizations, while others could deserve much less attention. If an organization makes a detailed analysis of the existing and potential risks, followed by a coherent and comprehensive plan of managing them inside and outside the organization, appointing appropriate resources and measures for this purpose, it could be in a better position to deal with environmental turbulence and its consequences. Additionally, although environmental turbulence is a central factor that influences organizations' CSRM, pressures can also come from internal challenges as well as from external stakeholders such as regulators or funders. Future studies could consider more factors and compare their different effects and role in the proposed model. Moreover, as risk behavior is influenced by several factors, future research may also put a stronger focus on the acting individuals in the social-cultural context being directly exposed to the risk and the role of people's experiences, values, and trust in institutions in this regard.

In conclusion, this study adds to the body of knowledge on CSRM, its antecedents and consequences. It addresses how different types of turbulences (market and technological turbulence) impacts CSRM and, in turn, organizational resilience. The results show that CSRM contributes strongly to organizational resilience and market and technological turbulences represent important antecedents in driving organizations' efforts regarding CSRM. In line with previous research, this study shows that (CS)RM enhances business performance, here organizational resilience. Our recommendations should invite decision-makers to put greater emphasis on CSRM.

CRediT authorship contribution statement

Susanne Durst: Conceptualization, Investigation, Methodology, Validation, Writing – original draft, Writing – review & editing. **Christoph Hinteregger:** Data curation, Formal analysis, Visualization, Writing – original draft, Writing – review & editing. **Malgorzata Zieba:** Funding acquisition, Investigation, Methodology, Writing – original draft, Writing – review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgements

The study was supported by a research grant from the National Science center (Poland) in the context of a research project 'Knowledge risks in modern organizations' (No. 2019/33/B/HS4/02250).

References

Aebi, V., Sabato, G., Schmid, M., 2012. Risk management, corporate governance, and bank performance in the financial crisis. J. Bank. Financ. 36 (12), 3213–3226.
Alahmari, A., Duncan, B., 2020. Cybersecurity risk management in small and medium-sized enterprises: a systematic review of recent evidence. In: Proceedings of the 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). Dublin, Ireland, pp. 1–5. https://doi.org/10.1109/CyberSA49311.2020.9139638.
Alvarez, S.A., Busenitz, L.W., 2001. The entrepreneurship of resource-based theory. J. Manage. 27 (6), 755–775.
Andersson, T., Cäker, M., Tengblad, S., Wickelgren, M., 2019. Building traits for organizational resilience through balancing organizational structures. SJM 35 (1), 36–45.
Aven, T., 2019. The call for a shift from risk to resilience: what does it mean? Risk Anal. 39 (6), 1196–1203.
Barnett, J., Breakwell, G.M., 2001. Risk perception and experience: hazard personality profiles and individual differences. Risk Anal. 21, 171–178. https://doi.org/10.1111/0272-4332.211099.
Barney, J., 1991. Firm resources and sustained competitive advantage. J. Manage. 17 (1), 99–120. https://doi.org/10.1177/014920639101700108.
Barney, J.B., 2001. Is the resource-based " view " a useful perspective for strategic management research? Yes. Acad. Manage. Rev. 26 (1), 41–56.
Bentler, P.M., Bonett, D.G., 1980. Significance tests and goodness of fit in the analysis of covariance structures. Psychol. Bull. 88 (3), 588–606.
Benz, M., Chatterjee, D., 2020. Calculated risk? A cybersecurity evaluation tool for SMEs. Bus. Horiz. 63 (4), 531–540.
Bodlaj, M., Čater, B., 2019. The impact of environmental turbulence on the perceived importance of innovation and innovativeness in SMEs. J. Small Bus. Manage. 57, 417–435.
Bubeck, P., Botzen, W.J.W., Aerts, J.C.J.H., 2012. A review of risk perceptions and other factors that influence flood mitigation behavior. Risk Anal. 32 (9), 1481–1495.
Burnard, K., Bhamra, R., 2011. Organisational resilience: development of a conceptual framework for organisational responses. Int. J. Prod. Res. 49 (18), 5581–5599.
Burton, R.M., Eriksen, B., Hakonsson, D.D., Snow, C.C, 2006. Organization Design: The Evolving State-of-the-Art, 6. Springer.
Calantone, R., Garcia, R., Dröge, C., 2003. The effects of environmental turbulence on new product development strategy planning. J. Prod. Innov. Manage. 20 (2), 90–103.
Callahan, C., Soileau, J., 2017. Does Enterprise risk management enhance operating performance? Adv. Account. 37, 122–139. https://doi.org/10.1016/j.adiac.2017.01.001.
Chowdhury, N., Gkioulos, V., 2021. Cyber security training for critical infrastructure protection: a literature review. Comput. Sci. Rev. 40, 100361.
Christensen, C.M., 1993. The rigid disk drive industry: a history of commercial and technological turbulence. Bus. Hist. Rev. 67 (4), 531–588.
Coden, M., Reeves, M., Pearlson, K., Madnick, S., & Berriman, C. (2023). An Action Plan for Cyber Resilience. MITSloan Management Review, 4 January 2023.
Colicchia, C., Creazza, A., Menachof, D.A., 2019. Managing cyber and information risks in supply chains: insights from an exploratory analysis. Supply Chain Manage. 24 (2), 215–240. https://doi.org/10.1108/SCM-09-2017-0289.
Committee of Sponsoring Organizations of the Treadway Commission (2017) Enterprise Risk Management Integrating with Strategy and Performance Executive Summary, https://www.coso.org/Shared%20Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf, accessed 14.05.2023.
Crovini, C., Ossola, G., Britzelmaier, B., 2021. How to reconsider risk management in SMEs? An advanced, reasoned and organised literature review. Eur. Manage. J. 39 (1), 118–134.
De la Peña Zarzuelo, I., 2021. Cybersecurity in ports and maritime industry: reasons for raising awareness on this issue. Transp. Policy (Oxf) 100, 1–4.
Dellana, S., Rowe, W.J., Liao, Y., 2022. A scale for measuring organizational risk management maturity in the supply chain. Benchmarking 29 (3), 905–930. https://doi.org/10.1108/BIJ-11-2020-0578.
Droge, C., Calantone, R., Harmancioglu, N., 2008. New product success: is it really controllable by managers in highly turbulent environments? J. Prod. Innov. Manage. 25 (3), 272–286.
Durst, S., Hinteregger, C., Zieba, M., 2019. The linkage between knowledge risk management and organizational performance. J. Bus. Res. 105, 1–10. Elsevier.
Edirisinghe Vincent, N., Pinsker, R, 2020. IT risk management: interrelationships based on strategy implementation. Int. J. Account. Info. Manage. 28 (3), 553–575. https://doi.org/10.1108/IJAIM-08-2019-0093.
El Baz, J., Ruel, S., 2021. Can supply chain risk management practices mitigate the disruption impacts on supply chains' resilience and robustness? Evidence from an empirical survey in a COVID-19 outbreak era. Int. J. Prod. Econ. 233, 107972.
Eling, M., McShane, M., Nguyen, T., 2021. Cyber risk management: history and future research directions. Risk Manage. Insurance Rev. 24 (1), 93–125.
Etale, A., Ammann, P., Siegrist, M., 2022. The influence of socio-economic status on risk prioritisation. J. Risk Res. 25 (4), 501–519. https://doi.org/10.1080/13669877.2021.1958046.
European Commission, Directorate-General for Migration and Home Affairs (2022) SMEs and cybercrime – Summary, Publications Office of the European Union, https://data.europa.eu/doi/10.2837/89101.
Farrell, M., Gallagher, R., 2019. Moderating influences on the ERM maturity-performance relationship. Res. Int. Bus. Finance 47, 616–628.
Fehle, F., Tsyplakov, S., 2005. Dynamic risk management: theory and evidence. J. Financ. Econ. 78 (1), 3–47.
Ferguson, M.E., Drake, M.J., 2021. Teaching supply chain risk management in the COVID-19 Age: a review and classroom exercise. Decision Sci. J. Innov. Educ. 19 (1), 5–14. https://doi.org/10.1111/dsji.12230.
Foli, S., Durst, S., & Temel, S. (2022). The link between supply chain risk management and innovation performance in SMEs in turbulent times. J. Entrepreneurship Emerg. Econ., Vol. ahead-of-print No. ahead-of-print.
Gates, S., Nicolas, J.-L.Paul, Walker, P.L, 2012. Enterprise risk management: a process for enhanced management and improved performance. Manage. Account. Q. 13 (3), 28–38.
Georgiadou, A., Mouzakitis, S., Askounis, D., 2022. Working from home during COVID-19 crisis: a cyber security culture assessment survey. Secur. J. 35 (2), 486–505.
Gordon, L.A., Loeb, M.P., Tseng, C.Y., 2009. Enterprise risk management and firm performance: a contingency perspective. J. Account. Public Policy 28 (4), 301–327.
Henrie, M., 2013. Cyber security risk management in the SCADA critical infrastructure environment. Eng. Manage. J. 25 (2), 38–45. https://doi.org/10.1080/10429247.2013.11431973.
Islam, J., Hu, H., 2012. A review of literature on contingency theory in managerial accounting. Afr. J. Bus. Manage. 6 (15), 5159–5164. https://doi.org/10.5897/AJBM11.2764.
ISO/IEC (2012). ISO/IEC 27032:2012(en) Information technology - Security techniques -Guidelines for cybersecurity. Available at https://www.iso.org/obp/ui/#iso:std:iso-iec: 27032:ed-1:v1:en.
Jaworski, B.J., Kohli, A.K., 1993. Market orientation: antecedents and consequences. J. Mark. 57 (3), 53–70.
Jiang, Y., Ritchie, B.W., Verreynne, M.L., 2019. Building tourism organizational resilience to crises and disasters: a dynamic capabilities view. Int. J. Tourism Res. 21 (6), 882–900.
Jin, C., Liu, A., Liu, H., Gu, J., Shao, M., 2022. How business model design drives innovation performance: the roles of product innovation capabilities and technological turbulence. Technol. Forecast. Soc. Change 178, 121591.
Ganin, A.A., Quach, P., Panwar, M., Collier, Z.A., Keisler, J.M., Marchese, D., Linkov, I., 2020. Multicriteria decision framework for cybersecurity risk assessment and management. Risk Anal. 40 (1), 183–199.
Gatzert, N., Schubert, M., 2022. Cyber risk management in the US banking and insurance industry: a textual and empirical analysis of determinants and value. J. Risk Insur. 89 (3), 725–763.
Gaurav, A., Gupta, B.B., Panigrahi, P.K., 2022. A novel approach for DDoS attacks detection in COVID-19 scenario for small entrepreneurs. Technol. Forecast. Soc. Change 177, 121554. https://doi.org/10.1016/j.techfore.2022.121554.
Guthrie, J., 2001. High-involvement work practices, turnover, and productivity: evidence from New Zealand. Acad. Manag. J. 44, 180–190.
Hair Jr., J.F., et al., 1998. Multivariate Data Analysis With Readings. Prentice-Hall, Englewood Cliffs, NJ.
Hu, L.-T., Bentler, P.M., 1999. Cutoff criteria for fit indexes in covariance structure analysis: conventional criteria versus new alternatives. Struct. Eq. Model. 6 (1), 1–55. https://doi.org/10.1080/10705519909540118.
Hartono, B., Wijaya, D.F., Arini, H.M., 2019. The impact of project risk management maturity on performance: complexity as a moderating variable. Int. J. Eng. Bus. Manage. 11, 1847979019855504.
Hartono, B., Wijaya, D.F.N., Arini, H.M., 2014. An empirically verified project risk maturity model: evidence from Indonesian construction industry. Int. J. Managing Projects Bus. 7 (2), 263–284. https://doi.org/10.1108/IJMPB-03-2013-0015.
Hoffmann, P., Schiele, H., Krabbendam, K., 2013. Uncertainty, supply risk management and their impact on performance. J. Purchasing Supply Manage. 19 (3), 199–211.
Hoppe, F., Gatzert, N., Gruner, P., 2021. Cyber risk management in SMEs: insights from industry surveys. J. Risk Finance 22 (3/4), 240–260.
Kline, R.B., 2010. Principles and Practice of Structural Equation Modeling, 3rd edn. Guilford Press, New York, USA.
Korosteleva, J., 2022. The implications of Russia's invasion of Ukraine for the EU energy market and businesses. British Journal of Management 33 (4), 1678–1682.
Kure, H.I., Islam, S., Mouratidis, H., 2022. An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. Neural. Comput. Appl. 34 (18), 15241–15271.
Lee, I., 2021. Cybersecurity: risk management framework and investment cost analysis. Bus. Horiz. 64 (5), 659–671.
Leiner, D.J., 2017. Our research's breadth lives on convenience samples a case study of the online respondent Pool 'SoSci panel. SCM 5 (4), 367–396.
Linnenluecke, M.K., 2017. Resilience in business and management research: a review of influential publications and a research agenda. Int. J. Manage. Rev. 19, 4–30. https://doi.org/10.1111/ijmr.12076.
Lundqvist, S.A., 2015. Why firms implement risk governance – Stepping beyond traditional risk management to enterprise risk management. J. Account. Public Policy 34 (5), 441–466.
Luo, Z., Callaert, J., Zeng, D., & Looy, B.V. (2022). Knowledge recombination, environmental turbulence and firms' innovation quality: the evidence from Chinese

pharmaceutical industry. European Journal of Innovation Management, Vol. ahead-of-print No. ahead-of-print. doi:10.1108/EJIM-10-2021-0517.
Luthans, F., Stewart, T.I., 1977. A general contingency theory of management. Acad. Manage. Rev. 2 (2), 181–195.
Madrid-Guijarro, A., Garcia, D., Van Auken, H., 2009. Barriers to Innovation among Spanish Manufacturing SMEs. J. Small Bus. Manage. 47 (4), 465–488.
Marshall, T.M., 2020. Risk perception and safety culture: tools for improving the implementation of disaster risk reduction strategies. Int. J. Disaster Risk Reduction 47, 101557.
Marsh & McLennan (2018). By the Numbers: global Cyber Risk Perception Survey. February 2018. https://www.marsh.com/pr/en/services/cyber-risk/insights/the-global-risks-report-201811.html.
Meyer, A.D., 1982. Adapting to environmental jolts. Adm. Sci. Q. 27, 515–537.
Meszaros, J., Buchalcevova, A., 2017. Introducing OSSF: a framework for online service cybersecurity risk management. Comput. Secur. 65, 300–313.
Mikes, A., 2009. Risk management and calculative cultures. Manage. Account. Res. 20 (1), 18–40.
Miller, T., Staves, A., Maesschalck, S., Sturdee, M., Green, B., 2021. Looking back to look forward: lessons learnt from cyber-attacks on industrial control systems. Int. J. Crit. Infrastruct. Prot. 35, 100464.
Mitchell, T., & Harris, K. (2012). Resilience: a risk management approach. ODI Background Note, 1–7.
Munir, M., Jajja, M.S.S., Chatha, K.A., Farooq, S., 2020. Supply chain risk management and operational performance: the enabling role of supply chain integration. Int. J. Prod. Econ. 227, 107667.
Oliveira, K., Méxas, M., Meirino, M., Drumond, G., 2019. Critical success factors associated with the implementation of enterprise risk management. J. Risk Res. 22 (8), 1004–1019.
Ovans, A., 2015. What resilience means, and why it matters. Harv. Bus. Rev. 5, 1–5.
Pratono, A.H., 2016. Strategic orientation and information technological turbulence: contingency perspective in SMEs. Bus. Process Manage. J. 22 (2), 368–382. https://doi.org/10.1108/BPMJ-05-2015-0066.
Proença, D., Estevens, J., Vieira, R., Borbinha, J.L., 2017. Risk management: a maturity model based on ISO 31000. In: Proceedings of the 2017 IEEE 19th Conference on Business Informatics (CBI), 01, pp. 99–108.
Puriwat, W., Hoonsopon, D., 2022. Cultivating product innovation performance through creativity: the impact of organizational agility and flexibility under technological turbulence. J. Manuf. Technol. Manage. 33 (4), 741–762. https://doi.org/10.1108/JMTM-10-2020-0420.
Qiu, L., Hu, D., Wang, Y., 2020. How do firms achieve sustainability through green innovation under external pressures of environmental regulation and market turbulence? Bus. Strat. Environ. 29 (6), 2695–2714.
Radanliev, P., De Roure, D., Page, K., et al., 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 3 (13). https://doi.org/10.1186/s42400-020-00052-8.
Radović, M.M., 2018. Organisational resilience and business continuity: theoretical and conceptual. JEBR 1 (1), 5–11.
Richard, P.J., Devinney, T.M., Johnson, G., 2009. Measuring organizational performance: towards methodological best practice. J. Manage. 35 (3) https://doi.org/10.1177/0149206308330560.
Rodríguez-Sánchez, A., Guinot, J., Chiva, R., López-Cabrales, Á., 2021. How to emerge stronger: antecedents and consequences of organizational resilience. J. Manage. Org. 27 (3), 442–459.
Sawalha, I.H.S., 2015. Managing adversity: understanding some dimensions of organizational resilience. Manage. Res. Rev. 38 (4), 346–366. https://doi.org/10.1108/MRR-01-2014-0010.
Settembre-Blundo, D., González-Sánchez, R., Medina-Salgado, S., et al., 2021. Flexibility and resilience in corporate decision making: a new sustainability-based risk management system in uncertain times. Global J. Flexible Syst. Manage. 22 (Suppl 2), 107–132. https://doi.org/10.1007/s40171-021-00277-7.
Shaikh, F.A., Siponen, M., 2023. Information security risk assessments following cybersecurity breaches: the mediating role of top management attention to cybersecurity. Comput. Secur. 124, 102974.
Siggelkow, N., Rivkin, J.W., 2005. Speed and search: designing organizations for turbulence and complexity. Org. Sci. 16 (2), 101–122.
Silva, E.S., Wu, Y., Ojiako, U., 2013. Developing risk management as a competitive capability. Strat. Change 22 (5–6), 281–294.
Singh, N., 2022. Developing business risk resilience through risk management infrastructure: the moderating role of big data analytics. Info. Syst. Manage. 39 (1), 34–52. https://doi.org/10.1080/10580530.2020.1833386.
Sjöberg, L., Moen, B.E., & Rundmo, T. (2004). Explaining risk perception. An evaluation of the psychometric paradigm in risk perception research, 10(2), 665-612.
Smith, D., Fischbacher, M., 2009. The changing nature of risk and risk management: the challenge of borders, uncertainty and resilience. Risk Manage. 11, 1–12. https://doi.org/10.1057/rm.2009.1.
Song, M., Droge, C., Hanvanich, S., Calantone, R., 2005. Marketing and technology resource complementarity: an analysis of their interaction effect in two environmental contexts. Strat. Manage. J. 26 (3), 259–276.
Statista (2023). Average total cost per data breach worldwide 2020-2022, by industry https://www.statista.com/statistics/387861/cost-data-breach-by-industry/, access 14.05.2023.
Staw, B.M., Sandelands, L.E., Dutton, J.E., 1981. Threat rigidity effects in organizational behavior: a multilevel analysis. Adm. Sci. Q. 26, 501–524.
Sturm, S., Hohenstein, N.O., Birkel, H., Kaiser, G., Hartmann, E., 2022. Empirical research on the relationships between demand- and supply-side risk management practices and their impact on business performance. Supply Chain Manage. 27 (6), 742–761. https://doi.org/10.1108/SCM-08-2020-0403.
Sun, W., Govind, R., 2017. Product market diversification and market emphasis: impacts on firm idiosyncratic risk in market turbulence. Eur. J. Mark. 51 (7/8), 1308–1331. https://doi.org/10.1108/EJM-09-2016-0510.
Temel, S., Durst, S., 2021. Knowledge risk prevention strategies for handling new technological innovations in small businesses. VINE J. Info. Knowl. Manage. Syst. 51 (4), 655–673. https://doi.org/10.1108/VJIKMS-10-2019-0155.
Tsai, K.H., Yang, S.Y, 2014. The contingent value of firm innovativeness for business performance under environmental turbulence. Int. Entrepreneurship Manag. J. 10, 343–366. https://doi.org/10.1007/s11365-012-0225-4.
Tsohou, A., Karyda, M., Kokolakis, S., Kiountouzis, E., 2015. Managing the introduction of information security awareness programmes in organisations. Eur. J. Info. Syst. 24 (1), 38–58. https://doi.org/10.1057/ejis.2013.27.
Viscelli, T.R., Beasley, M.S., Hermanson, D.R., 2016. Research insights about risk governance: implications from a review of ERM research. Sage Open 6 (4), 2158244016680230.
Wall, T., Michie, J., Patterson, M., Wood, S., Sheehan, M., Clegg, C., West, M., 2004. On the validity of subjective measures of company performance. Pers. Psychol. 57, 95–118.
Wang, G., Dou, W., Zhu, W., Zhou, N., 2015. The effects of firm capabilities on external collaboration and performance: the moderating role of market turbulence. J. Bus. Res. 68 (9), 1928–1936.
Wang, Y., Zeng, D., Di Benedetto, C.A., Song, M., 2013. Environmental determinants of responsive and proactive market orientations. J. Bus. Indus. Market. 28 (7), 565–576. https://doi.org/10.1108/JBIM-10-2011-0156.
Wilden, R., Gudergan, S.P., 2015. The impact of dynamic capabilities on operational marketing and technological capabilities: investigating the role of environmental turbulence. J. Acad. Market. Sci. 43, 181–199. https://doi.org/10.1007/s11747-014-0380-y.
Willumsen, P., Oehmen, J., Stingl, V., Geraldi, J., 2019. Value creation through project risk management. Int. J. Project Manage. 37 (5), 731–749.
Zhao, Y., Cavusgil, E., Cavusgil, S.T., 2014. An investigation of the black-box supplier integration in new product development. J. Bus. Res. 67 (6), 1058–1064.

Susanne Durst is a full professor of management at the Department of Business Administration at Reykjavik University (Iceland) and a full professor of business administration at the University of Skövde, Sweden. Her research interests include knowledge (risk) management, innovation management, responsible digitalization, and sustainable business development in the context of small entrepreneurial companies. She has been conducting several national and international research projects. Her work has been awarded different awards and published in international peer-reviewed journals. Before joining academia, she worked with private enterprises.

Christoph Hinteregger earned his Ph.D. at the School of Management at University of Innsbruck, Austria. His-research interests include corporate entrepreneurship, organisational culture, and human resource management.

Malgorzata Zieba is an Associate Professor of Management at the Department of Management, Faculty of Management and Economics at Gdańsk University of Technology. Her research areas concern knowledge and innovation management in SMEs, mainly from the knowledge-intensive business services (KIBS) sector. She has attracted funding from the Ministry of Science and Higher Education and the National Science center in Poland. She was a Junior Fellow at the University of Glasgow, Scotland in 2012. She has published several papers on knowledge management in journals such as Journal of Knowledge Management, Journal of Business Research or Engineering Economics and presented research results at international conferences.