IMPRESAPROGETTO
ELECTRONIC JOURNAL OF MANAGEMENT
n. 1 – 2023

Organizational resilience: state of the art and new future cyber inquiries

Martina Neri*, Federico Niccolini†, Francesco Virili‡

Summary: 1. Introduction – 2. Method – 2.1 Eligibility: inclusion and exclusion criteria – 2.2 Information sources – 2.3 Items collection – 2.4 Protocol and final sample description – 3. Analysis and discussion – 3.1 RQ1: OR conceptualizations – 3.2. RQ2: OR key features – 3.2.1 before the event – 3.2.2 During the event – 3.2.3 After the event – 3.3 RQ3: OR as a property – 3.4 RQ4: Events associated with OR – 3.5 A 3 stages time-based conceptual framework of OR – 3.6Future research direction: understanding cyber OR – 4. Conclusion

Abstract

Contemporary societies, and the organizational systems on which they rely, are increasingly exposed to unexpected disruptive events, such as the recent health or geo-political crises. Organizations therefore need a certain level of Organizational Resilience (OR). Since OR is a multifaceted concept, a first aim of this article is to find a *trait d'union* among many studies and conceptualizations of OR, stimulating academic debate, critical thinking, and further research. An additional goal is to propose a specific direction for future research leading to a better understanding of the characteristics that make organizations more resilient to an increasing relevant adverse phenomenon, namely cybersecurity and related cyberattacks. The authors develop a systematic literature review about the concept of OR in the Management and Organization science fields. A second facet is the authors' proposed three-stage conceptual framework of OR, which is consistent with the relevant ideas emerging from the systematic literature review. A third section focuses on the exploration of relationships between cybersecurity and organizational domains, going beyond a purely technical focus.
Results show that there is a need to address many unresolved research gaps, and to systematize the fragmentation of current Organization and Management research. It is clear

*Martina Neri, Ph.D Candidate, Department of Business and Management, University of Pisa, E-mail: martina.neri@phd.unipi.it
† Federico Niccolini, Associate Professor of Organization Science, Department of Political Sciences, Univerisity of Pisa, E-mail: federico.niccolini@unipi.it
‡ Francesco Virili, Associate Professor of Organization Science, Department of Business and Law, Catholic University of the Sacred Hearth, E-mail: Francesco.virili@unicatt.it

Received 6th February 2023; accepted 12th May 2023.
DOI: 10.15167/1824-3576/IPEJM2023.1.1543

that many critical areas still lack a solid and more comprehensive operationalization of OR, including cyber OR.

Keywords: organizational resilience; cybersecurity; systematic literature review.

1. Introduction

Contemporary societies, and the organizational systems they rely on, are increasingly exposed to unexpected disruptive events. Societies are facing both new and old disruptive events, especially so during the last decade, according to the Global Risk Report released by the World Economic Forum in 2023. The most recent of these are Covid-19 and the war in Ukraine. These events have re-enacted a series of disruptive events, such as inflation, cost of living crisis, trade wars, and widespread social unrest. Indeed, "the environment surrounding organizations increasingly challenges them by posing different threats in various forms from both inside and outside an enterprise's boundaries" (Annarelli and Nonino, 2016, p. 2). Organizational Resilience (OR) has become a necessity for enterprises operating in this increasingly dynamic and turbulent environment. The OR perspective implies a broad and radical proactive approach that extends beyond the idea of a preventive focus, via activities that anticipate (Somers, 2009) whether a potentially harmful event will occur. Organizations that adopt a more proactive approach to their environment (Ates and Bititci , 2011) arise stronger and more resourceful than before (Vogus and Sutcliffe, 2007), according to the logic of learning and change (Duchek, 2020).

Several research and practical fields, including ecology (Folke et al., 2010; Holling, 1973), psychology (Youssef and Luthans, 2007), and engineering (Hollnagel et al., 2006), have a long tradition of engaging with OR. However, the concept has only recently gained recognition in the Management and Organizational Sciences. Although notable research efforts have been made in these fields, a certain degree of fragmentation still affects the OR notion. As a starting point, we depict the most recent and relevant literature reviews on the concept of OR. Due to their significance, we used these works to initiate an in-depth understanding of the work that has been done so far, and the objectives informing it. This allowed us to shape this study's contribution more effectively. Table 1 summarizes the focus, method, and output of the three main research items.

Table n. 1 – Systematic literature reviews on the concept of OR

Literature review	Objective	Method	Output
Hillmann and Guenther (2021)	Analysis of the resilience concept, focusing on both the operational and conceptual issues	Systematic Literature Review	Conceptual integrative model based on resilient behavior, resources, and capabilities. These main concepts enable the resilient response and related organizational growth
Linnenluecke (2017)	Identify both knowledge development and gaps in business and management research on resilience	Systematic Literature review	Outline key research streams and future research direction and opportunities
Spagnoletti and Za (2021)	Understand the concept of digital resilience, integrating both the Normal Accident Theory (NAT) and High-Reliability Organization (HRO) research area	Bibliometric analysis	Identify declining and emerging NAT and HRO contributions. The authors propose a set of key concepts to build an integrated framework of resilience in digitally enabled operations

Source: personal elaboration

These significant contributions advanced the current understanding and knowledge of the OR concept. Compared to these research outputs, this study focuses on a different facet and proposes a different outcome. The framework proposed here focuses on the time dimension of OR, rather than on behaviors, capabilities, and resources (Hillmann and Guenther, 2021), thus engaging with a different conceptual perspective. This research does not embrace specific theories to be applied to the concept of resilience, including the digital one (Spagnoletti and Za, 2021). However, we claim that NAT (Normal Accidents Theory) and HRO (High Reliability Organizations) theories lay a solid foundation for a theoretical understanding of cyber resilience. Although the objective is similar to that of Linnenluecke (2017), our research takes a step back and is limited to the OR fragmentation issue, thus not covering perspectives such as supply chain resilience.

As a result, this study has the objective of determining the current state of organizational research on OR and proposes a specific future direction for research on the cybersecurity phenomenon. The contribution of this work is to find a *trait d'union* across organizational studies' conceptualizations of resilience, and to stimulate debate, critical thinking, and further research. This will open new avenues for detecting, measuring, monitoring, and improving organizational resilience.

To reach this goal, our research is based on a systematic literature review (Jesson et al., 2011). The paper is organized as follows: We first describe the method used in the systematic literature review. Then we emphasize the state of the art, and propose new research questions, all in line with both the research question and its aim. We also propose a conceptual framework for OR that is consistent with the relevant ideas emerging from the literature analysis.

2. Method

We took some key steps to assure methodological rigor, transparency, and reproducibility, in line with the goal of a systematic literature review (Jesson et al., 2011). Below are the steps that we performed during this systematic review.

The first step in this study focused on defining the elements that would guide the systematic literature review search. The authors established the research questions that the literature review aims to address. To perform a systematic literature review it is necessary to formulate answerable questions which help to clarify the terminology and scope of the research (Papaioannou et al., 2016). The research questions allow us to focus on and define the research scope, and find the relevant literature associated with it. The research questions focus on the investigation of the conceptual nature of OR. This yielded the following detailed questions:

RQ1: What are the different conceptualizations of OR?
RQ2: Which are the key features related to OR?
RQ3: What properties are associated with OR conceptualizations?
RQ4: To which kind of event are the conceptualizations of OR linked?

As stated before, a certain degree of dispersion still surrounds the OR concept. This research focuses on tracing the major key features emerging from the systematic literature review.

2.1 Eligibility: inclusion and exclusion criteria

The authors established a set of explicit selection criteria for a study to be included. These are:

A) The study is a scientific paper (article or review), book or a book chapter, or conference proceedings[1]. Considering the fragmentation and dispersion of the OR literature, the authors set out to include different document typologies;
B) The authors did not set a time cut off for database research;
C) The study is in its final stage of publication;
D) The study is written in English;
E) Due to the extensive body of literature regarding OR in different scientific areas (e.g., Ecology and Psychology), it was necessary to define the research strictly to the Organizational Sciences or Business and Management area. This is because there are many different research areas that draws on OR with different ontological ideas (Hillman, 2021) and different setting (Sawalha, 2015). Although the focus is on organizations, and the ways in which they deal with resilience, this

[1] Book, book chapter and conference proceedings are included in the sample only if they are relevant (i.e. they have more than 100 citations).

research does not focus on a specific type of organization if it is outside the current research scope.

The authors also established a set of additional exclusion criteria. A document is included in the final sample if OR is focal in the study, as well as if OR is conceptualized at the organizational level. Although the systematic literature review research focused on the management and organization science areas, the disciplinary intersection regarding OR made the identification of additional exclusion criteria worthwhile. Hence, a document is not included in the sample if refers to OR at the individual level (e.g., psychological resilience), macro level (e.g., nations' or cities' resilience), or if OR is a sub- or side concept. Although considerable management research draws on individual traits of employees as a source of OR (DesJardine et al., 2019), we focus on the organizational level of analysis, because "organizational resilience is neither an aggregate of individual resilience nor a subset of field or industry resilience" (Hepfer and Lawrence, 2022, p. 2).

Table 2 offers a synthesis of inclusion and exclusion criteria applied both to first screening and full document scoping. When an examined contribution did not satisfy these criteria, it was not included in the final sample.

Table n. 2 – Set of inclusion and exclusion criteria

Type of criteria	Set of criteria
Inclusion	scientific paper (article or review), book or a book chapter, conference proceedings.; final stage of publication; written in English; Organizational Sciences or Business and Management area
Exclusion	OR is focal in the study; OR is not a sub or a side concept; OR is conceptualized at the organizational level

Source: personal elaboration

Besides the use of inclusion and exclusion criteria, the authors followed an ancestry approach (i.e., footnote chasing) (Cooper, 1982). We used citations from relevant studies to track down earlier research on which the studies are based (i.e., the ancestors). This was done to prevent us from omitting relevant studies. Since there is a studies fragmentation around OR, some of the most relevant studies do not strictly relate to the covered areas. These are thus likely to be left out, resulting in a lack of essential contributions on OR conceptualization. Although this could be seen as a disadvantage, it is worth noting that using a systematic approach is valuable to ensure the transparency and reproducibility of the research.

2.2 Information sources

To perform the research, the authors used EBSCO Business Source Complete and Scopus. Due to the significant differences between the two databases, the terms were searched in two different but equal ways.

In EBSCO Business Source Complete, we based the research on "subject term research", with the subject term OR. There was no need to limit the scope of the research to a specific research area, since the database specializes in business and management sciences. In Scopus, the research was performed using Boolean operators applied to title, abstract, and keyword. The Boolean operators reflect the inclusion criteria discussed above, as stated in TITLE-ABS-KEY ("organizat* resilien*" OR "organisat* resilien*") AND (LIMIT-TO (SRCTYPE , "j") OR LIMIT-TO (SRCTYPE , "b")) AND (LIMIT-TO (PUBSTAGE , "final")) AND (LIMIT-TO (DOCTYPE , "ar") OR LIMIT-TO (DOCTYPE , "re") OR LIMIT-TO (DOCTYPE , "ch")) AND (LIMIT-TO (LANGUAGE , "English")). It was necessary to use both organisation and organization, due to different spelling of the words; and we used the asterisk to include synonyms, such as organizational, organization, resilient, and resiliency, as keywords.

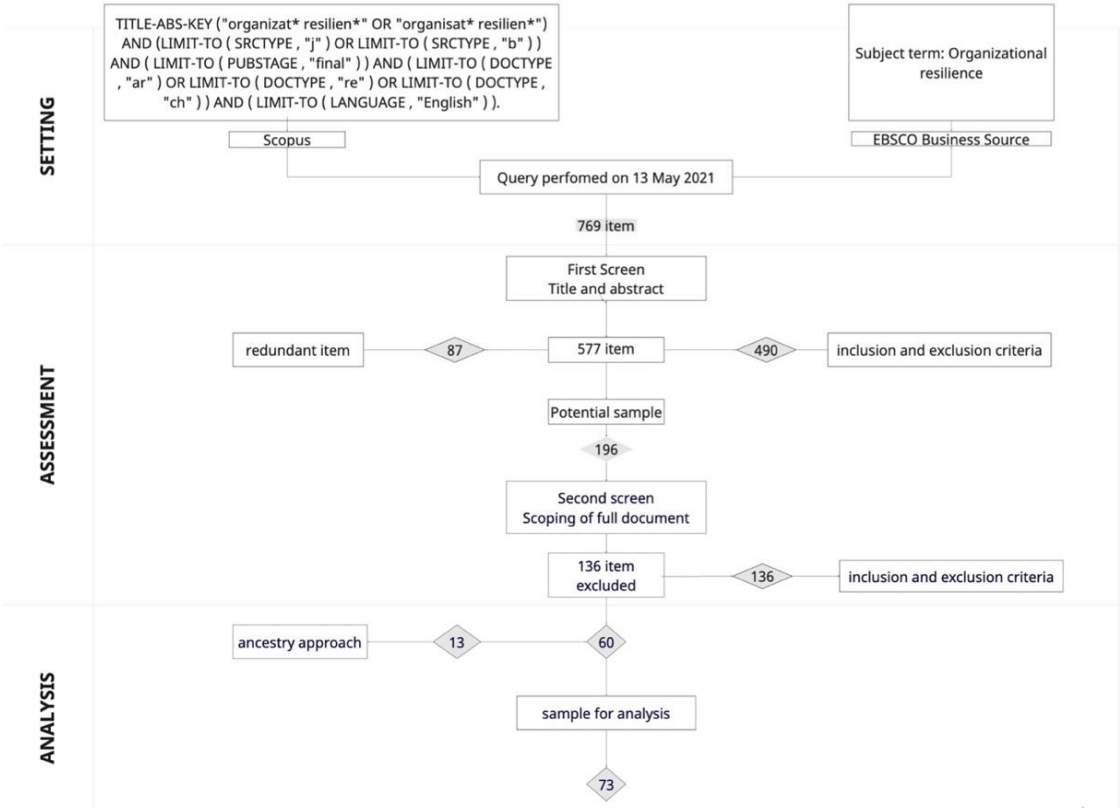
We did the keyword search multiple times in both databases to find the ideal selection of keywords and Boolean operators. We recorded all the database queries. The number of documents extracted, as well as the combination of keywords and Boolean operators, are included in the record. Access to the documents was provided by the authors' university digital library or was obtained via open access.

2.3 Items collection

As Figure 1 shows, the query returned a set of 769 potentially relevant documents. We divided the assessment phase of this study into two document screenings that both took the exclusion criteria into account. The authors evaluated a document's relevance based on a detailed examination of its title and abstract. A total of 87 documents were excluded because they were redundant. When we added the full document to the scope for inclusion, a first set of 490 documents were excluded because they did not comply with the criteria. We then did the second screening and scoped the full document. All 196 remaining documents were extensively examined to ensure that they include all or most of the information required for this study. As a result of this process, another 136 items were excluded. Following the ancestry approach, we added 13 items to the final sample. The final dataset includes 73 documents.

Figure 1 describes the flow and number of documents obtained from the research.

Figure n.1 – Systematic literature review process (source: personal elaboration)



Source: personal elaboration

2.4 Protocol and final sample description

The authors developed a review protocol to be followed to categorize all the documents included in the final sample for the analysis phase. The protocol ensures a rigorous classification of the OR concept, and was of fundamental value when used as a checklist to assess a document's satisfaction of both inclusion and exclusion criteria. The protocol also ensures the reproducibility of the research. We sorted the protocol into three categories. The bibliographic section includes details, such as the journal's name and ranking, the abstract and keywords, year, and type of publication. Consequently, we classified the documents into those that used qualitative, quantitative, and mixed methods. We added a brief explanation of the methodology used for each of these. The section on the construct of OR identifies the nature of the concept (entity or property), the event that triggers OR, and its key attributes. This

section was valuable to fully explore the conceptual nature of OR and develop the proposed conceptual framework. Table 3 summarizes the review protocol we used to analyze the final sample of documents.

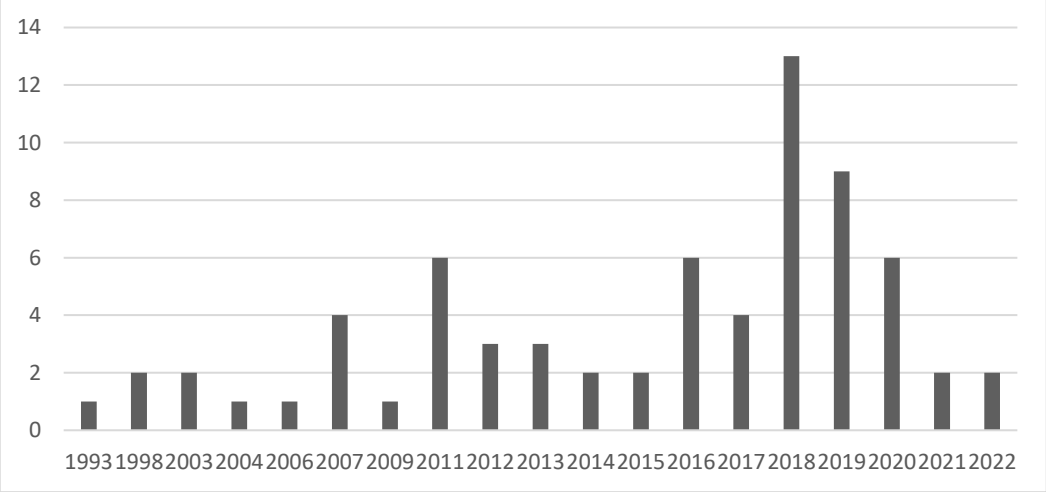
Table n. 3 – Research protocol categories' synthesis (source: personal elaboration)

Systematic Literature Review protocol	Description
Bibliographic	Authors; Year; Title; Abstract; Journal; Journal ranking; Keywords; Review Process; Nr citations; Origin; Country; Institution; Discipline; Type of publication
Study content	Objective; Research question/hypothesis; Results; Study design; Methodology
OR nature	Nature of the concept (entity and property); Key attributes; Type of event associated to OR

Source: personal elaboration

The final sample's descriptive analysis already pointed out some interesting avenues of inquiry. Several documents were published more recently than others, which is consistent with the recent increase in managerial and organizational perspectives in the study of the phenomena of resilience at the organizational level. The number of documents obtained for each year is shown in Graph 1.

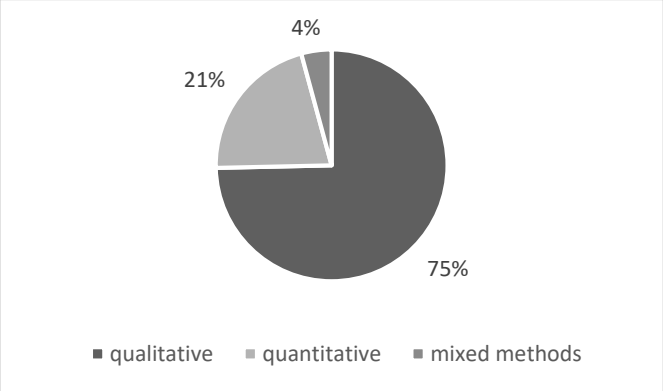
Graph n. 1. Number of documents obtained for each year



Source: personal elaboration

When we examined the study design, an assessment of the documents provided more discussion contents. Most of the documents cover qualitative methods. Notable research efforts have been made to operationalize resilience, either through variables or measurement scales (Gittel et al., 2006; Mafabi et al., 2012; Prayag et al., 2018). However, it is still necessary to consolidate measures or variables that may be used both before and after an event to gain more insight into OR and its nature. The percentage of documents utilizing each methodology is shown in Graph 2.

Graph n. 2 - Percentage of documents utilizing each methodology



Source: personal elaboration

In section 2 we provide an analysis and discussion following the research question that guided this systematic literature review. We also propose a 3 staged time-based conceptual framework as a synthesis – and a source – for future research on and operationalization of OR.

3. Analysis and discussion

3.1 RQ1: OR conceptualizations

The authors start by addressing RQ1: What are the different conceptualizations of OR? For convenience of exposure, only the explicit definitions are shown in the table below.

Contributions that focus on defining the key features of OR, but do not propose an explicit definition, will be discussed later in this section. Table 4 outlines the ways in which OR is conceptualized based on the findings of the systematic literature review.

Table n. 4 – explicit OR conceptualization

Author(s)	OR conceptualization
Horne and Orr, (1998)	a fundamental quality of individuals, groups, organizations, and systems as a whole to respond productively to significant change that disrupts the expected pattern of events without engaging in an extended period of regressive behavior
Coutu (2002)	capacity to be robust under conditions of enormous stress and change.
Vogus and Sutcliffe (2007)	maintenance of positive adjustment under challenging conditions such that the organization emerges from those conditions strengthened and more resourceful
Hamel and Valikangas (2004)	a capacity for continuous reconstruction. It requires innovation with respect to those organizational values, processes, and behaviors that systematically favor perpetuation over innovation. Strategic resilience is not about responding to a onetime crisis. It's not about rebounding from a setback. It's about continuously anticipating and adjusting to deep, secular trends that can permanently impair the earning power of a core business. It's about having the capacity to change before the case for change becomes desperately obvious
Lengnick-Hall and Bell (2005)	a unique blend of cognitive, behavioral, and contextual properties that increase a firm's ability to understand its current situation and to develop customized responses that reflect that understanding
McManus et. al., (2007)	a function of an organisation: situation awareness, management of keystone vulnerabilities and adaptive capacity, in a complex, dynamic and interconnected environment
Somers (2009)	it is more than mere survival; it involves identifying potential risks and taking proactive steps to ensure that an organization thrives in the face of adversity
Lengnick-Hall et al., (2011)	the firm's ability to effectively absorb, develop situation- specific responses to, and ultimately engage in transformative activities to capitalize on disruptive surprises that potentially threaten organization survival
Linnenluecke et al., (2012)	organizational capacity to absorb the impact and recover from the actual occurrence of an extreme weather event
Ates and Bititci (2011)	the ability to anticipate key opportunities and events from emerging trends, constantly adapting and changing, rapidly bouncing back from disaster and remaining stable in a turbulent environment
Chewning et al., (2013)	it rests in the ability of the affected parties to communicate and reorganize across periods of rapid change or chaos. It involves the ability to respond to situations as well as to adapt in terms of creating new solutions
Whitman et. al., (2013)	an organization's ability to plan for, respond to and recover from emergencies and crises
Limnios et al., (2014)	the magnitude of disturbance the system can tolerate and still persist
Mafabi et. al., (2012)	it is measured in terms of organizational adaptation, organizational competitiveness, and organizational value

Ortiz-de-Mandojana and Bansal (2016)	the ability of organizations to anticipate, avoid, and adjust to shocks in their environment
Annarelli and Nonino (2016)	the organization's capability to face disruptions and unexpected events in advance thanks to the strategic awareness and a linked operational management of internal and external shocks. The resilience is static, when founded on preparedness and preventive measures to minimize threats probability and to reduce any impact that may occur, and dynamic, when founded on the ability of managing disruptions and unexpected events to shorten unfavorable aftermaths and maximize the organization's speed of recovery to the original or to a new more desirable state
Clement and Rivera (2017)	it is a relatively stable quality that is put to the test once a discontinuity occurs and a firm adapts to return to its original equilibrium
DesJardine et. al., (2019)	it is assessed through two organizational outcomes of general environmental shocks: the severity of organizational losses and the organization's time to recovery
Hillman et. al., (2018)	this capacity consists of organizational capabilities by which firms anticipate trends and threats, make sense of and cope effectively with unexpected events, and adapt to changes to develop a dynamic capability that is directed toward facilitating strategic change
Kahn et. al., (2018)	the organization's ability to absorb strain and preserve or improve functioning despite the presence of adversity
Ma et al., (2018)	an organizational capability to survive in, adapt to, bounce back from and often thrive in unexpected, sometimes disastrous events and, in more broad sense, turbulent environments
Jiang et al., (2019)	an organization's ability to persist and withstand external environmental changes (preparation), mitigate and cope with negative effects caused by the changes (response), and bounce forward to a new state for better future performance (recovery)
Conz and Magnani (2020)	it is a dynamic attribute of the firm characterized by a) a proactive phase at time (t-1); an absorptive or adaptive phase at time t, and b) a reactive phase at time (t+1), where t is the time when an unexpected event occurs and alters the equilibrium of the firm
Hillman and Guenther (2021)	is the ability of an organization to maintain functions and recover fast from adversity by mobilizing and accessing the resources needed. An organization's resilient behaviors, resilience resources and resilience capabilities enable and determine organizational resilience. The result of an organization's response to adversity is growth and learning

Source: personal elaboration

In keeping with these conceptualizations, three major OR concepts arise.

The first conceptualization looks at OR as "respond and recover". Horne and Orr (1998) discuss responding productively to significant change; Linnenluecke et al., (2012) focus on the idea of absorbing the impact and recovering; and Lengnick-Hall and Bell (2005) respond with developing customized and specific responses to the event.

The second concept focuses on "adaptation and adjustment". According to Vogus and Sutcliffe (2003), OR relies on the maintenance of a positive adjustment under the challenging conditions.

The third notion conceptualizes OR as "anticipation". Somers (2009) states that OR is related to the identification of potential risk. Ortiz-de-Mandojana and Bansal (2016) also conceptualize OR as the ability to anticipate, avoid, and adjust to shocks.

All three concepts these are redundant in many OR conceptualizations. However, it is worth noting that most of the explicit conceptualizations offer a broader perspective, since they may have multiple connotations.

Whitman et al. (2013) based their conceptualization on plan, respond and recover. Ma et al., (2018) found OR in survive, adapt, and bounce back. Annarelli and Nonino (2016) go beyond a conceptualization solely based on quality and properties by including a static and dynamic perspective of OR.

This difference in conceptualization also reflects the temporal dimension of OR. Indeed, many of the conceptualizations emphasize an own, unique timeframe. While some authors focus on the moments prior to the event, others stress the idea of the moments during the event, and yet others the moments following the event. Some ther conceptualizations, on the contrary, encompass all three moments and can be outlined as more holistic. According to this analysis, OR seems to be related to a certain degree of temporality.

Key OR features appear to be related to different points in time; some features exist and must be implemented before the event occurs, while others ensure a positive response when the event occurs. Finally, other ex-post activities are concerned with change and learning as a result of the event.

3.2. RQ2: OR key features

According to this viewpoint, the main features of OR are depicted here in three distinct stages. It is worthwhile to consider whether the three stages are distinct in time or if they are part of a larger iterative system, such as the event's life cycle.

We now outline the main findings of the systematic literature review related to OR key features. We distinguish the key features according to the specific point in the three-step timeframe at which they manifest themselves or need to be implemented, in line with the emerging conceptual framework. Consistent with this approach, we frame key features of OR in three moments in time, namely before, during, and after the event. We thus address RQ2: Which are the key features related to OR?

3.2.1 Before the event

Before the event occurrence, OR is linked to the development of consciousness about the organizations' environment. Situational awareness, defined as a measure of the organization's understanding and perception of its entire operating environment (McManus et al., 2007), is crucial in this perspective. Environmental scanning and the

recognition of environmental fluctuations (Burnard and Bhamra, 2011) are key features to be developed. To realize this aim, monitoring and simulating activities should be implemented that will enable the organization to detect unexpected events sooner (Vogus and Sutcliffe, 2007). These elements are functional to resilience and are not devoted to eliminate errors or unexpected events instead (Weick and Sutcliffe, 2007). According to Ortiz-de-Mandojana and Bansal (2016), an organization should quickly interpret signals from the environment to avoid escalation of a situation. Burnard et al. (2018) point out that "the continual monitoring of environmental fluctuations allows the organization to adapt its operations effectively through an active situational awareness process" (p. 357). Parker and Ameen (2018) suggest that an organization's search for information about disruptive events could result in more information to be used to plan appropriate responses. Many of these features are included in the broad categories of observation and identification by Duchek (2020).

While it is critical to monitor the external environment, it is also essential to understand the internal organizational one. In this regard, vulnerability assessment plays an important role. McManus et al. (2007) focus on management of keystone vulnerabilities. These are organizational aspects, whether managerial or operational, that can have a negative impact when a crisis results from an unexpected event. According to Burnard and Bhamra (2011), "understanding not only the requirements of a given organizational system, but also the system vulnerability is essential in developing a proactive approach to threat mitigation and enhancing an organization's adaptive capacity (p. 5591)". The analysis of possible vulnerabilities is also proposed by Vogus and Sutcliffe (2007) as one of the five mindful, interrelated organizing behavioral processes. According to Aanestad and Jensen (2016), "mindful organizations perform well, both in anticipating, and in containing, the unexpected" (p. 15).

Planning strategies are essential to manage vulnerabilities in the business environment (Lee et al., 2013). Accoding to Darkow (2019), "by improving planning capabilities, organizations become more resistant, and the likelihood of potentially dangerous situations turning into crises decreases (p. 150)". Planning activities also rely on services availability and asset functioning while dealing with an unexpected event (Wood et al., 2019). Planning strategies include a wide range of actions and tools, such as a Business Continuity Plan or Recovery Plan (Duchek, 2020).

While OR appears to be related to a specific set of planned actions (Pal et al., 2014; Branicki et al., 2017; Prayag et al., 2018), it is worth noting that "organizations prepare without knowing if, when, or where an unexpected event will occur in the future" (Duchek, 2020, p. 227). According to this approach, the unexpected component of an event also becomes relevant.

When an unexpected event occurs, there is always a limited amount of information available, regardless of planning strategies. An attitude of wisdom is seen as a source of resilience in such situations, since "wise people know that they don't fully understand what is happening right now, because they have never seen precisely this event before" (Weick, 1993, p. 641). Wisdom enables an organization's leaders to doubt the validity and exhaustivity of beliefs, values, knowledge, information, abilities, and skills (Weick, 1993).

Resilient organizations should promote a tolerance for uncertainty and taking decisions with less information than is desirable (Mallak, 1998). According to this viewpoint, organizations should encourage and train for "bricolage" (Mallak, 1998; Weick, 1993), i.e., create solutions by using whatever tools or materials are available, and not necessarily waiting until they have the 'correct' or 'proper' ones (Coutu, 2002). Consistent with this perspective, Somers (2009) embraces the idea that organizations with a high resilience level are the ones that systematically train employees to improvise solutions. Improvisation allows them to immediately replace the collapsed organizational order (Weick, 1993).

Employees also play a role in OR via knowledge and team composition. Expansion of the group knowledge base enables organizations to increase the addition of new knowledge to memory (Vogus and Sutcliffe, 2003). Lengnick-Hall et al. (2011) suggest that organizations should hire employees to "ensure [that] a range of different experiences, perspectives, paradigms, and competencies are available in the workforce" (p. 249). According to Duchek (2020), a broader form of work-group diversity could enhance OR, and may result in increased sensemaking (Weick, 1993) and decision making (Legnick-Hall et al., 2011). According to Linnenluecke et al. (2012), anticipatory adaptation relies on past experiences and sensemaking. A high value placed on individual difference (Lengnick-Hall et al., 2011) enables the existence of teams with different fields of expertise and different capacities. This may result in increased problem solving in difficult situations (Vogus and Sutcliffe, 2003). Moreover, the different perspectives provided by interactions when new employees are added to decision-making processes, can also enable OR (Vogus and Sutcliffe, 2007). According to Van der Vegt et. al. (2015), "whereas the composition of individual characteristics determines the system's potential for resilience, the relationships between individual employees and the social network in which these individuals are embedded strongly determine the availability and accessibility of these capabilities and resources for adaptive responses" (p. 973). Lengnick-Hall and Beck (2005) stress that a deep social capital provides an "interpersonal foundation for thriving despite uncertainty and for developing rapid responses to emerging conditions" (p. 752).

Adequate resources appear to be a fundamental feature that ensures being prepared for an unexpected event. In the description of their conceptualization of OR, Conz and Magnani (2020) stress the idea of resourcefulness and redundancy. Resourcefulness is defined as an attribute to be implemented in the adaptive resilience path before the event occurs. Resourcefulness relies on accumulating different resources (e.g., physical, human, or financial) (Branicki et al., 2017; Pal et al., 2014). Redundancy relies on the absorptive OR path and underlines the necessity of keeping resources in reserve. Management of sufficient resources also provides extra capacity to operate during a crisis (Lee et al., 2013) and to absorb unexpected changes (Chowdhury et al., 2019). In general, organizations with abundant resources could access and use a varied "toolkit" that enables them to respond effectively to and resist an unexpected event (Van der Vegt et al., 2015). According to Lengnick-Hall et al. (2011), "access to broad resource networks is a key element in creating contextual conditions that support resilience development (p. 247)". This also underlines the

necessity of external resources, such as those provided by relationships and suppliers. According to Mallak (1998), "external resource adequacy encompasses resources of advice, information, finances, emotional support, and practical help" (p.5). External resources could promote slack and diversity, thus enabling action inventory and an improved attitude to challenging conditions over assumptions (Lengnick-Hall and Beck, 2005).

3.2.2 During the event

When the event occurs, organizational structure plays a fundamental role. According to Lengnick-Hall et al. (2011), "resilient organizations are not managed hierarchically" (p. 247). This is because "organizational structure serves as a barrier towards organizational resilience" (Mallak, 1998, p. 7). Expanded decision making boundaries (Mallak, 1998), decentralized decision making and a high degree of permeability between organizational boundaries (Burnard and Bhamra, 2011), and minimization of silos (Lee et al., 2013), are all necessary for a decentralized and less formalized organizational structure. Key positions should be generalist in nature, to ensure their ability to fulfill multiple roles (Somers, 2009). If an employee is not able to respond to a specific situation, there should be other people that could fill the role (Chowdhury et al., 2019). This is possible when an individual shares the vision of a team's mission (Mallak, 1998). Furthermore, employees need to address problems without minimal supervision intervention (Somers, 2009). All these features are necessary to ensure adaptive responses during a crisis (van der Vegt et al., 2015). Although there is a need for autonomy, leadership plays a vital role in ensuring adaptive responses during a crisis (Chowdhury et al., 2019). According to Teo et al. (2017), leaders activate resilience via relational connections that result in new connections, collective meaning-making and sensemaking, and emotional resources. It is worth noting that an organization should find stability in balancing processes of normative control and power distribution (Andersson et al., 2019).

While dealing with a crisis, organizations should make tough decisions quickly (Chowdhury et al. 2019; Lee et al., 2013) by implementing ad hoc solutions (Duchek, 2020). Employees should have access to resources as needed and develop a critical understanding of the situation (Somers, 2009). Agility, the capacity to recognize and use opportunities quickly while dealing with unexpected turbulence in the environment, is fundamental to achieve this aim (Bouaziz and Hachicha, 2018). This means taking rapid action, developing alternatives to benefit from negative circumstances, and taking the required action in a nimble manner (Bouaziz and Hachicha, 2018; Kantur and Iseri-Say, 2015). These features also concern the change and renewal of the strategies implemented by organizations. Hamel and Valikangas (2004) state that OR "requires alternatives as well as awareness—the ability to create a plethora of new options as compelling alternatives to dying strategies" (p. 3).

Even if organizations have to use their knowledge in novel ways (Chowdhury et al., 2019; Lee et al., 2013;), the maintenance of core asset functions and service availability while dealing with a disturbance is equally important (Darkow, 2019;

Wood et al., 2019). Conz and Magnani (2020) state that OR conceptualization, robustness and adaptability are necessary to achieve this aim. Indeed, robustness is the capability to resist shocks by preventing and reducing the effects of variables that can make a firm vulnerable in its operating environment. According to Bouaziz and Hachicha (2018), robustness relies on the ability to stand straight and preserve position, generate diverse solutions, resist loss, and continue on a path. Adaptability is the ability to adjust the firm's response and internal processes to changing external conditions (Conz and Magnani, 2020). Both capabilities are included in the absorptive and adaptive resilience path. Park and Ameen (2018) stress the importance of resource reconfiguration, which is the ability to manage and reconfigure resources in response to changes in the environment, as a source of better performance and survival.

3.2.3 After the event

After the event, change and learning are the key features of OR (Burnard and Bhamra, 2011; Duchek, 2020; Pal et al., 2014). Organizations learn from past events and engage in a double loop feedback to reinforce their capabilities (Vogus and Sutcliffe, 2007). According to Burnard and Bhamra (2011), organizations can learn and develop new knowledge because of a resilient response, thus enabling advanced monitoring of the environment. Organizations "must be able to reflect on the crisis situation and to incorporate the gained insight into the existing knowledge base" (Duchek, 2020, p. 230). Lee et al. (2013) stress that organizations should incorporate lessons learned into its future projects. Reflective practices (Lengnick-Hall and Beck, 2011), taking the time to learn from experience (Parker and Ameen, 2018), and feedback analysis (Duchek, 2020) are functional to this aim. According to Hillman et al. (2018), "combined learning intervention positively influences the development of anticipation capabilities. Specifically, it improves recognition and enhances the capabilities of individuals to understand the "big picture" and anticipate a broader spectrum of developments at different levels within the organization" (p. 482). It is worth noting that OR "relies upon past learning and fosters future learning, but exists independently of learning activities in that resilience represents a broader store of capabilities" (Vogus and Sutcliffe, 2007, p. 3418). In addition, more research is needed to understand how organizations learn and develop new capacity after an unexpected event (Linnenluecke et al., 2012).

Learning is also narrowly related to change, since it is fundamental to gain overall change and develop new norms, values, and beliefs (Duchek, 2020). Wood et al. (2019) foreground adaptation as the use of new knowledge from the event, altering protocols, configuring the system, training personnel, and other aspects to become more resilient.

However, organizations reach their adaptation limit at a certain point (Dow et al., 2013; Clement, 2017). According to Linnenluecke et al. (2012), resilience is related to "rapidly unfolding and/or unexpected events (surprises)", while adaptation refers

only to an expected event (p. 22). This discussion gives rise to the important OR question of the degree of unexpectedness of the event.

The post-event phase also focuses attention on recovery activities that help organizations to operate again (Darkow, 2019). Additionally, the long-term recovery perspective enhances the organization's ability to learn from and be prepared for future adverse situations (Christianson et al., 2009).

Positive perception of experiences and positive adaptive behaviors are also highlighted in the post-event phase (Mallak, 1998). This includes viewing change as an opportunity and forming a positive and constructive perception of the problem. The propensity to find meaning from adverse conditions implies a strong organizational value system (Coutu, 2002).

3.3 RQ3: OR as a property

Most studies that we analyzed that describe what it is that makes an organization resilient, focus on OR key features or elaborate a novel OR conceptualization. A life-or-death paradigm of organizations may be too extreme to describe the consequences of an event. Hence, it is worth asking what makes an organization non-resilient. Are non-resilient organizations those that do not have the features described so far? Or do other features make an organization less or non-resilient? To these aims, solid empirical operationalization of OR should be developed. The phases described so far are closely linked to each other, which means that OR is a process in which each phase reinforces the next and thus operates as a double loop feedback. While accepting the concept of OR as a process, it is also necessary to focus on the properties associated with OR. In reporting on this focus, the authors address RQ3: What properties are associated with OR conceptualizations?

In line with the evidence of the systematic literature review, it is evident that OR may include many different properties. OR manifests itself as a quality, a capability, and an ability, as well as a capacity. Hence, the literature has not reached an agreement about which of these, or what combination of them, is the correct one. A definition of these terminologies would be useful. Indeed, if we examine the definitions of ability and capability, we note that they have different intended meanings. While ability usually refers to possessing a certain degree of skills, a capability refers to a potential scenario. Capacity, in its turn, refers to the potential for doing something. This discussion relates to the organization's life-or-death paradigm, in which different levels of OR may be conceivable if OR is expressed through degrees. This could potentially imply that organizations may be more or less resilient depending on the OR features they implement. The concept of a potential scenario additionally reinforces the idea of resilience as a latent concept that reveals itself (only) when the event occurs.

Table 5 summarizes the properties associated with OR in previous conceptualizations.

Table n. 5 – Property associated with OR

References	Property
Clement and Rivera (2017), Horne and Orr (1998)	quality
Coutu (2002), Linnenluecke et al., (2012)	capacity
Ates (2011), Chewning et al., (2012), Jiang et al., (2019), Kahn et al., (2018), Lengnick-Hall and Beck (2005), Lengnick-Hall et al., (2011), Whitman (2013)	ability
Burnard and Bhamra (2011), Burnard et. al., (2018)	ability and capability
Annarelli and Nonino (2016), Hillman et. al., (2018), Ma et. al., (2018), Sullivan-Taylor and Branicki (2011),	capability
Conz and Magnani (2020)	dynamic attribute

Source: personal elaboration

3.4 RQ4: Events associated with OR

The authors then focused on RQ4: To which kind of event are the conceptualizations of OR linked? Indeed, the "resilience of what" issue is still unsolved (Pinheiro et al., 2022). The following discussion revolves around the depiction of the events associated with OR.

Table 6 summarizes the main events associated with OR gleaned from previous conceptualizations.

Each reference expresses the event through a different conceptualization. However, there is an overlap between them (e.g., certain conceptualizations are manifestations of others). A certain kind of fuzziness is therefore noted, and an agreement is still far from being reached (Darkow, 2019). Operationalizing OR solely according to this perspective could arguably be reductive. Indeed, each event has its distinctive characteristics and leads to different impacts. It is also worth noting that different events involve greater or lesser degrees of unexpectedness. For instance, a so-called "black swan event" (a random event with a large impact, incomputable probabilities, and surprise effects (Taleb, 2007) has been used to explain the pandemic scenario. Since Covid-19 and attendant events (e.g., an increase in cyberattacks) are associated with OR, it is reasonable to wonder whether black swan features define the event triggering OR. It is, however, more accurate to assume that the two events have quite different characteristics. In reality, several features of the suggested conceptual framework, such as environmental monitoring and vulnerability assessment, can consistently reduce the level of unexpectedness of a cyberattack and its implications. In this regard, Hamel and Valikangas (2004) state

that "even "unexpected" shocks can often be anticipated if one is paying close attention" (p. 3). As Hepfer and Lawrence (2022) point out, there is still a need to understand "whether OR developed in relation to one type of adversity will lead to greater resilience in relation to other types of adversity" (p. 22). Is it therefore reasonable to state that organizations that exhibit a greater resilience to the pandemic will exhibit a greater resilience to cyberattacks? Will the organization become more resilient overall, or will there be a specific resilience event path?

Table n. 6 – Events associated with OR

Reference	Event
Horne and Orr (1998)	significant change
Linnenluecke et al. (2012)	extreme event
Lengnick-Hall et al. (2011)	disruptive surprises
Ates (2011)	disaster
Vogus and Sutcliffe (2003; 2007)	challenging conditions
Somers (2009), Kahn et. Al., (2018)	adversity
Sullivan-Taylor and Branicki (2011)	extreme event
Burnard and Bhamra (2011)	turbulence/discontinuities
Bhamra et. al., (2011)	disruptions
Chewing et. al., (2012)	rapid change/chaos
Ortiz-de-Mandojana and Bansal (2016)	shocks in their environment
Whitman et. al., (2013)	emergencies and crises
Annarelli and Nonino (2016)	disruptions and unexpected events
Limnios et al. (2014)	disturbance
Clement and Rivera (2017)	discontinuity
Teo et. al., (2017)	exougenous shock
Hillman et al., (2018)	unexpedcted events/changes
Ma et. al., (2018)	dasaustrous events
Coutu (2002)	stress and change

Source: personal elaboration

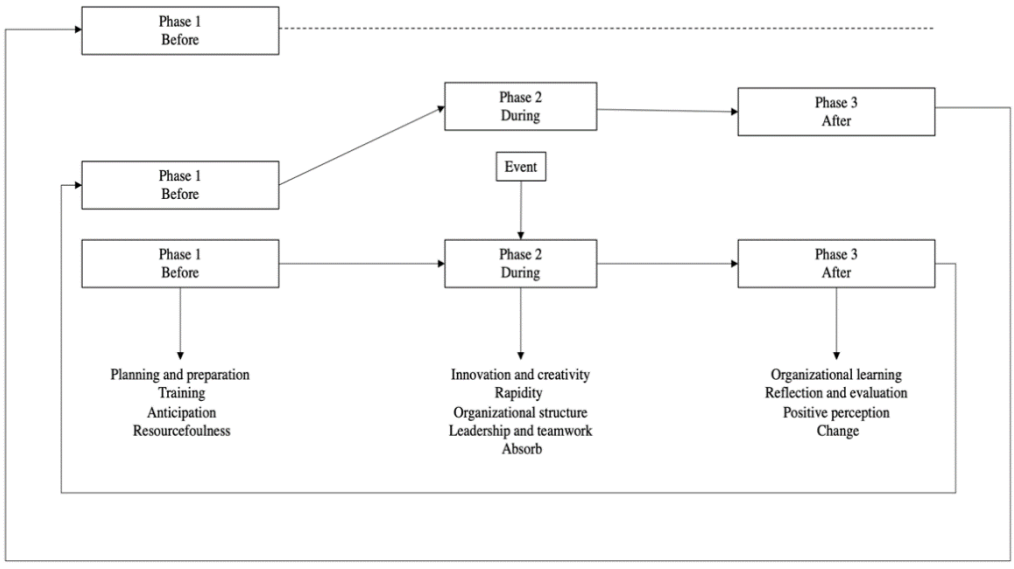
It is also important to note that "a specific form of adversity may have significantly different impacts on different organizations" (Hepfer and Lawrence, 2022, p. 8). For instance, the agricultural sector may be more directly impacted by extreme weather events than the financial industry. Similarly, a cyberattack might have a more direct impact on organizations that handle critical information (e.g., patents or industrial plans).

3.5 A 3 stages time-based conceptual framework of OR

In line with the previous discussion, we support the idea that "a more precise elaboration could clarify the impacts of different kinds of adversity and their potential for triggering OR and its various empirical manifestations" (Pinheiro et al., 2022, p. 11). According to this discussion, as stated before We thus present a future research proposal for the understanding of cyber OR in the last section.

Figure 2 summarizes the three-stages conceptual framework that we propose here as a synthesis of the literature review.

Figure n. 2 – The organizational resilience loop – A three-stage conceptual framework of OR



Source: personal elaboration

The conceptual framework proposed here embraces the idea of OR as a three-stage process, where OR manifests itself as a dynamic property in each of the main stages. The OR features are implemented or manifest themselves in different ways in different stages.

The three stages appear to align to an event's life cycle. This is consistent with the results of the systematic literature review. Indeed, some conceptualizations of OR seem to refer to a specific stage of the framework, while others emphasize a specific moment in time; and the key features that emerge from them can often be linked to each of the three stages discussed above. This conceptual framework embraces the idea that OR not only allows an organization to bounce back to the pre-event state (Ates, 2011; Clement and Rivera, 2017), but that it also enables the organization to learn and grow and thus emerge more powerful and resourceful than before (Duchek, 2020; Lengnick-Hall et al., 2011). The new knowledge derived from the third phase could be interpreted as a facilitator of the first stage. Anticipation and planning activities could be improved through change and learning because the organization is supposed to reflect on the event to fully understand what was expected to happen and what actually happened, and to highlight mistakes that were made, or opportunities that were seized. The novel experience will converge in a new improved phase 1. This might happen through improved planning and training initiatives, for instance.

Following this discussion, a certain degree of connection and interdependence between the stages should be assumed. The proposed conceptual framework states that OR exists before and after an event, but it manifests itself only when triggered by an event. Due to this latent nature, it may seem as if it is impossible to attribute OR before the organization faces an adverse event (Darkow, 2019; Hepfer and Lawrence, 2022). However, with the proposed conceptual framework we argue that OR should be implemented and enacted during each of the three phases, because each one is correlated with the others so that none of them can exist without the others, making all three necessary to constitute a resilient organization. A focus on the key features of each phase and their interrelationship could be useful to strengthen the theorical foundation of OR and grounding its inner nature.

3.6 Future research direction: understanding cyber OR

Cyber OR is a growing and evolving issue for many organizations. Evidence from different reports affirms that cyber threats continue to affect organizations of all sizes (WEF, 2022; Verizon Report, 2020). The actual pandemic now constitutes one of the most impactful scenarios since World War II. This is especially true for cybersecurity issues; indeed, “cybersecurity failure is one of the risks that worsened the most through Covid-19” (WEF, 2022, p. 48). The Covid-19-related social distancing rules provided a massive acceleration of the digital revolution, increasing the use of the Internet for all types of activities in many parts of the world and for people of all ages. Many businesses must adjust and adapt because of the increased use of IT and digital tools. Likewise, “the pandemic has brutally exposed fundamental weaknesses and

limits in the way organizations engage with digitalization" (Faraj, 2021, p. 2). Global cybercrime costs are expected to increase by 15 per cent per year over the next five years, reaching $10.5 trillion annually by 2025 (Morgan, 2020). Furthermore, cyberattacks are increasingly sophisticated, targeted, and coordinated (Farwell and Rohozinski, 2011), and take full advantage of many vulnerabilities, including human error. A total of 95% of cybersecurity issues can be traced to human error, while insider threats, whether intentional or accidental, represent 43% of all breaches (WEF, 2022).

According to this perspective, cybersecurity refers to the protection of computer networks to preserve the "Confidentiality, Integrity, and Availability (the so-called CIA triad)" of resources (hardware, software, firmware, information or data, and telecommunications) in the information system (Onwubiko and Lenaghan, 2007). Whether it is a confirmed data breach in which the confidentiality of the data was compromised, or an integrity incident, such as altering the behavior of a person via phishing, the actions against the assets result in CIA-triad compromises.

The current authors go beyond the CIA-triad approach, in alignment with von Solms and van Niekerk (2013), and embrace the definition of cybersecurity as "the protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace" (p. 101). We propose focusing on the understanding of the inherent nature and meaning of cyber OR as a future research direction.

The current research on OR from a cyber perspective, or cyber resilience (CR), is mainly discussed in the engineering field, where a technical focus is prevalent, and the organizational perspective is not taken into consideration. Indeed, organization science is a new, yet promising field in the cybersecurity domain. In fact, in accordance with Dalal et al. (2022), we claim that it is worth focusing on the organizational aspects of cybersecurity, that is to say "the efforts organizations take to protect and defend their information assets, regardless of the form in which those assets exist, from threats internal and external to the organization" (p. 5). Indeed, even if the discussion about cybersecurity primarily focuses on the technical side, a new approach to cybersecurity is oriented at involving the management and organizational fields (Telay and Klein, 2021). The reason for this is that cybersecurity not only implies technological impacts, but also includes "almost every dimension of sustaining and growing a successful organization" (Telay and Klain, 2021, p. 1). The relationship that exists between cybersecurity and organization science, and specifically OR in this context, may also offer meaningful insights for future research. Developing a cyber OR perspective essentially requires a multidisciplinary approach and necessitates changes from the traditional conception of cybersecurity (Hult, et al. 2014). Organizations need a new approach directed not only to technologies, but also to learning through adverse events, thus evolving from a defensive or reactive attitude to a proactive one. A comprehensive cybersecurity strategy normally includes physical, procedural, logical, and organizational forms of protection (Baskerville et al., 2014; Swanson and Guttman, 1996). An environment in which

cybersecurity and information assets are protected by organizational actors, will hopefully improve the overall security of that organization (Dojkovski et al., 2007).

This discussion leads us to claim that there are at least three main pathways through which the two research domains (i.e., OR and CR) can become contaminated. One is purely related to the contents and related findings of this study. The second pertains to the potential contribution of organization sciences to cybersecurity research. Models and theories from the organizational sciences may offer several insights that would help to ground cyber OR. The third pathway investigates how cybersecurity can provide a new perspective in the comprehension of phenomena that have previously been extensively researched in organization sciences. Hence, there is more than one way for cross-contamination across these two different, but complementary, research areas.

Analysis of OR conceptualization in the literature review reveals a certain degree of temporality. We discovered three distinct temporal paths (either separately or combined) throughout the systematic literature review. in fact, the OR temporal dimension emerged as being somewhat fragmented. Future studies should focus on examining ways in which CR is conceptualized at the organizational level to investigate whether the temporal dimension can be detected as well.

This relates to the idea that a triggering event is needed for OR to be manifested. Indeed, the findings indicate that discussions of OR always outline events in a fragmented and generalized way. However, we already claimed that various events have different characteristics and impacts. Cyberattacks are often not experienced in the same way as other kinds of events (e.g., climate disasters). Generally speaking, the effect and impact of cyberattacks start before they are noticeable to the organization. As a result, the features that we have outlined here as requirements to respond to the event may not be adequate, suggesting a need for additional preventive measures. The framework we defined here can then be used in further research to examine how each key feature manifests itself in the specific event of a cyberattack. Since this field of study is still in its infancy, future research should move toward a qualitative and exploratory methodological approach.

The sort of cyberattack that an organization faces will be a major factor in this discussion. Indeed, some cyberattacks may exhibit a shifted, longer, or shorter time lag between infiltration and manifestation (e.g., malware versus phishing). This depends on how the cyberattack involves the human factor. Future research should focus on understanding the relevance and value of the time dimension in OR when confronted with a cyberattack.

The conceptual framework proposed here may be used as a solid foundation for future research aimed at identifying inconsistencies between these two research areas. The main aim should be to develop an integrated and holistic conceptual framework. A preliminary analysis of the CR concept reveals some interesting insights.

To face cybersecurity threats effectively, organizations need to develop an inter-organizational and networking approach, by specifically creating relationships with strategic partners and national authorities (Baskerville et al., 2014). Organizations with high cybersecurity levels recognize the relevant role of employee and machine

learning and training, and an organizational culture cognizant of cybersecurity. In fact, acting on organizational culture, and creating an extensive and systemic situational awareness perspective about potential threats is an accepted milestone within organizational cyber OR (Skopik et al., 2016).

All these fragmented elements appear to be in accordance with the findings of the systematic literature review, which suggests a certain degree of generalizability of the conceptual framework. However, to be operational cybersecurity needs an element of specialist knowledge often found in people employed on the technical side of an organization (Bell, 2017). This element may thus be inconsistent with the requirement that employees should be able to fill multiple roles. There are also some characteristics, like adaptation (Sepúlveda Estay et al., 2020), absorbing, planning, and preparation (Linkov et al., 2013), and diversity and flexibility (Heeks and Ospina, 2019) that emerge in both cybersecurity and OR literatures. However, the former field focuses on information systems, while the latter is concerned with the entire organization.

This discussion thus confirms and emphasizes the need for future research to propose an integrated conceptual framework by aligning the two perspectives. Academics and practitioners might also benefit from a more thorough understanding of the concept of cyber OR. On the one hand, an in-depth account of feature inconsistencies would provide a more precise elaboration and improved theoretical understanding of the concept of OR in the event of a cyberattack. On the other hand, defining and designing the practical features to be adopted to be resilient to a cyberattack would prove to be beneficial overall.

We move investigate how some of the organizational sciences' main constructs could shed light on cybersecurity and OR.

In this respect organizational learning is a meaningful construct that also emerges as relevant in the systematic literature review analysis. It would provide insight into the actual relevance of organizational learning in successfully managing the new knowledge generated in the post-event phase. Organizational learning could indeed be conceptualized as "the capability of an organization to process knowledge—in other words, to create, acquire, transfer, and integrate knowledge, and to modify its behavior to reflect the new cognitive situation, with a view to improving its performance" (Jerez-Gomez et al., 2003, p. 716). Effective cybersecurity requires an element of specialized knowledge; therefore, knowledge integration and hierarchical coordination implications could provide a further research opportunity (Grant, 1996). Following our conceptual framework, it is evident that training activities play an important role in preparing the organization to face an adverse event, such as a cyberattack. It could be useful to explore the relationship between training and risk aversion. Indeed, Dalal et al. (2022) indicate that training could lead to a misclassification of email (e.g., being suspicious of all emails), thus impeding job performance. Future research should be oriented to investigate the role of training effectiveness to explore the efficacy of cybersecurity training delivery methods (e.g., gamification, text, and video).

Organizational culture theories offer other interesting insights. It would be worthwhile to explore how organizational culture might positively influence OR.

Following Schein's (1985) model of organizational culture, cybersecurity culture is defined as "the beliefs, values, and attitudes that drive employee behaviors to protect and defend the organization from cyberattacks" (Huang and Pearlson, 2019, p. 6399). Future research should focus on the relationship between organizational culture in shaping and promoting cyber OR.

Moving on to the third future research path, we suggest that cybersecurity could also offer an important research avenue for organizational science. Indeed, cybersecurity provides an insight into two different types of employees, namely end-users and cybersecurity-focused employees. This distinction would enable a variety of future research inquiries, consequently going beyond the traditional categorization, e.g., by gender or age. In addition, training activities and their respective effectiveness could be investigated in relation to these two types of employees. This could also provide a new research focus and perspective on theories relating to job performance and satisfaction (Dalal et al., 2022). Future research could also focus on personal trait influencing the effectiveness of training, such as risk-taking propensity. Another promising future research avenue could be investigating what kind of slack resources (Gittell et al., 2006; Meyer, 1982) could enable the organization to face and resist to a cyberattack in the specific context of cyber OR, and in what ways it could effect this.

4. Conclusion

Different major concepts emerge from the OR literature, with each one describing OR as having key features relating to some, or all, of the three stages of the conceptual framework we proposed here. Tracking the current understanding of OR appears to be both complex and critical. The appealing, simple idea of "being able to resist and survive" reveals a much more complex construct.

The conceptual framework we propose offers a synthesis of the major relevant ideas emerging from the analysis, thus revealing a more comprehensive conceptualization. The literature analysis we performed in this study suggests that OR is a latent, multifaced construct. Besides, while OR manifests itself when triggered by an event, it exists before, during and after the event. This concept of OR suggests that being resilient means to be prepared and to plan for an event, to respond to the event, and to adapt to it, learn from it, and change according to it.

We emphasized that "any phenomena claiming resilience must remain within the limits that delineate the threshold of the concept. Those limits can be understood as threefold: the phenomena should extend over time, maintain a continuity of essence, and deal with serious adversity" (Young et al. 2022, p. 310). The first and the last limits (temporality and adverse events) are explicitly present in the proposed framework. The idea of continuity is only implicitly assumed in the current version of the framework, and a more extensive analysis of this aspect is among the many questions that still need to be addressed.

This research raises a slew of new questions. There is a need to address the many unresolved research gaps and to clarify the ambiguity of current research. Many

critical areas also still lack a solid and more comprehensive operationalization of OR (including cyber OR). Future research should focus on operationalizing OR, with the goal of not only understanding it better, but also suggesting promising managerial avenues for dealing with an increasingly risky and uncertain environment. In addition, a broad conceptual framework that considers the organizational and technical features that characterize OR and cyber resilience, should be developed.

References

Aanestad, M., & Jensen, T. B., (2016). Collective mindfulness in post-implementation IS adaptation processes. *Information and Organization, 26*(1-2), 13-27. https://doi.org/10.1016/j.infoandorg.2016.02.001.

Andersson, T., Cäker, M., Tengblad, S., & Wickelgren, M. (2019). Building traits for organizational resilience through balancing organizational structures. *Scandinavian Journal of Management, 35*(1), 36-45.

Annarelli, A., & Nonino, F. (2016). Strategic and operational management of organizational resilience: Current state of research and future directions. *Omega, 62*, 1–18. https://doi.org/10.1016/j.omega.2015.08.004

Ates, A., & Bititci, U. S. (2011). Change process: A key enabler for building resilient SMEs. *International Journal of Production Research, 49*(18), 5601-5618. https://doi.org/10.1080/00207543.2011.563825

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management, 51*(1), 138–151. https://doi.org/10.1016/j.im.2013.11.004

Bell, S. (2017). Cybersecurity is not just a 'big business' issue. *Governance Directions*, *69*(9), 536-539. https://www.governanceinstitute.com.au/resources/governance-directions/archive/issue-9/cybersecurity-is-not-just-a-big-business-issue/

Bouaziz, F., & Hachicha, Z. S. (2018). Strategic human resource management practices and organizational resilience. *Journal of Management Development, 37*(10), 537-551. https://doi.org/10.1108/JMD-11-2017-0358

Branicki, L. J., Sullivan-Taylor, B., & Livschitz, S. R. (2017). How entrepreneurial resilience generates resilient SMEs. *International Journal of Entrepreneurial Behavior & Research, 24*(7), 1244–1263. https://doi.org/10.1108/IJEBR-11-2016-0396

Burnard, K., & Bhamra, R. (2011). Organisational resilience: development of a conceptual framework for organisational responses. *International Journal of Production Research, 49*(18), 5581-5599. https://doi.org/10.1080/00207543.2011.563827

Burnard, K., Bhamra, R., & Tsinopoulos, C. (2018). Building organizational resilience: Four configurations. *IEEE Transactions on Engineering Management, 65*(3), 351-362. 10.1109/TEM.2018.2796181

Chewning, L. V., Lai, C. H., & Doerfel, M. L. (2013). Organizational resilience and using information and communication technologies to rebuild communication structures. *Management Communication Quarterly, 27*(2), 237-263. https://doi.org/10.1177/0893318912465815

Chowdhury, M., Prayag, G., Orchiston, C., & Spector, S. (2019). Postdisaster social capital, adaptive resilience and business performance of tourism organizations in Christchurch, New Zealand. *Journal of Travel Research, 58*(7), 1209-1226. https://doi.org/10.1177/0047287518794319

Christianson, M. K., Farkas, M. T., Sutcliffe, K. M., & Weick, K. E. (2009). Learning through rare events: Significant interruptions at the Baltimore & Ohio Railroad Museum. *Organization Science, 20*(5), 846–860. https://doi.org/10.1287/orsc.1080.0389

Clément, V., & Rivera, J. (2017). From adaptation to transformation: An extended research agenda for organizational resilience to adversity in the natural environment. *Organization & Environment, 30*(4), 346-365. https://doi.org/10.1177/1086026616658333

Clusit, (2021). *Rapporto sulla sicurezza ICT in Italia*. Milano: CLUSIT.

Conz, E., & Magnani, G. (2020). A dynamic perspective on the resilience of firms: A systematic literature review and a framework for future research. *European Management Journal, 38*(3), 400-412. 10.1016/j.emj.2019.12.004

Cooper, H. M. (1982). Scientific guidelines for conducting integrative research reviews. *Review of Educational Research, 52*(2), 291-302. https://doi.org/10.2307/1170314

Coutu, D. L. (2002, May). How resilience works. *Harvard Business Review, 80*(5), 46-56. https://hbr.org/2002/05/how-resilience-works

Dalal, R. S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S. J., & Brummel, B. J. (2022). Organizational science and cybersecurity: abundant opportunities for research at the interface. *Journal of Business and Psychology, 37*(1), 1-29. https://doi.org/10.1007/s10869-021-09732-9

Darkow, P. M. (2019). Beyond "bouncing back": Towards an integral, capability-based understanding of organizational resilience. *Journal of Contingencies and Crisis Management, 27*(2), 145-156. https://doi.org/10.1111/1468-5973.12246

DesJardine, M., Bansal, P., & Yang, Y. (2019). Bouncing back: Building resilience through social and environmental practices in the context of the 2008 global financial crisis. *Journal of Management*, *45*(4), 1434-1460. https://doi.org/10.1177/0149206317708854

Dojkovski, S., Lichtenstein, S., & Warren, M. J. (2007). Fostering information security culture in small and medium size enterprises: an interpretive study in Australia (pp. 1560-1571). *Proceedings of the 15th European Conference on Information Systems.* ECIS.

Dow, K., Berkhout, F., Preston, B. L., Klein, R. J., Midgley, G., & Shaw, M. R. (2013). Limits to adaptation. *Nature Climate Change, 3*(4), 305-307. https://doi.org/10.1038/nclimate1847

Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. *Business Research*, *13*(1), 215-246. https://doi.org/10.1007/s40685-019-0085-7

Estay, D. A. S., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber-resilience assessment frameworks. *Computers & security, 97*, 101996. 10.1016/j.cose.2020.101996

Faraj, S., Renno, W., & Bhardwaj, A. (2021). Unto the breach: What the COVID-19 pandemic exposes about digitalization. *Information and Organization*, *31*(1), 1-7. 10.1016/j.infoandorg.2021.100337

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, *53*(1), 23-40. https://doi.org/10.1080/00396338.2011.555586

Folke, C., Carpenter, S. R., Walker, B., Scheffer, M., Chapin, T., & Rockström, J. (2010). Resilience thinking: Integrating resilience, adaptability and transformability. *Ecology and Society*, *15*(4). http://www.ecologyandsociety.org/vol15/iss4/art20/

Gittell, J. H., Cameron, K., Lim, S., & Rivas, V. (2006). Relationships, layoffs, and organizational resilience: Airline industry responses to september 11. *Journal of Applied Behavioral Science, 42*(3), 300–329. https://doi.org/10.1177/0021886306286466

Grant, R. M. (1996). Toward a knowledge-based theory of the firm. *Strategic Management Journal, 17*(2), 109-122. https://doi.org/10.1002/smj.4250171110

Hamel, G., & Valikangas, L. (2004, May). The quest for resilience. *Icade. Revista de la Facultad de Derecho*, *62*, 355-358. https://revistas.comillas.edu/index.php/revistaicade/article/view/7226

Heeks, R., & Ospina, A. V. (2019). Conceptualising the link between information systems and resilience: A developing country field study. *Information Systems Journal*, *29*(1), 70-96. https://doi.org/10.1111/isj.12177

Hepfer, M., & Lawrence, T. B. (2022). The heterogeneity of organizational resilience: Exploring functional, operational and strategic resilience. *Organization Theory*, *3*(1), 1-29. https://doi.org/10.1177/26317877221074701

Hillmann, J. (2021). Disciplines of organizational resilience: Contributions, critiques, and future research avenues. *Review of Managerial Science, 15*(4), 879-936. 10.1007/s11846-020-00384-2

Hillmann, J., & Guenther, E. (2021). Organizational resilience: a valuable construct for management research?. *International Journal of Management Reviews, 23*(1), 7-44. https://doi.org/10.1111/ijmr.12239

Hillmann, J., Duchek, S., Meyr, J., & Guenther, E. (2018). Educating future managers for developing resilient organizations: The role of scenario planning. *Journal of Management Education, 42*(4), 461-495. https://doi.org/10.1177/1052562918766350

Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics, 4*, 1-23. https://doi.org/10.1146/annurev.es.04.110173.000245

Hollnagel, E., Woods, D. D., & Leveson, N. (2006). *Resilience engineering: Concepts and precepts.* Aldershot, UK: Ashgate.

Horne III, J. & Orr, J. (1998) Assessing behaviors that create resilient organizations. *Employment Relations Today*, *24*(4), 29-39.

Huang, K., & Pearlson, K. (2019, January). For what technology can't fix: Building a model of organizational cybersecurity culture. *Proceedings of the 52nd Hawaii International Conference on System Sciences.* Hawaii: HICSS.

Hult, F., & Sivanesan, G. (2014). What good cyber resilience looks like. *Journal of Business Continuity & Emergency Planning, 7*(2), 112-125.

Linnenluecke, M. K. (2017). Resilience in business and management research: A review of influential publications and a research agenda. *International Journal of Management Reviews*, *19*(1), 4-30.

Jerez-Gomez, P., Céspedes-Lorente, J., & Valle-Cabrera, R. (2005). Organizational learning capability: a proposal of measurement. *Journal of Business Research, 58*(6), 715-725. 10.1016/j.jbusres.2003.11.002

Jesson, J., Matheson, L., & Lacey, F. M. (2011). Doing your literature review: Traditional and systematic techniques. *Evaluation & Research in Education, 24*(3), 219-221. 10.1080/09500790.2011.581509

Jiang, Y., Ritchie, B. W., & Verreynne, M. L. (2019). Building tourism organizational resilience to crises and disasters: A dynamic capabilities view. *International Journal of Tourism Research, 21*(6), 882-900. https://doi.org/10.1002/jtr.2312

Kahn, W. A., Barton, M. A., Fisher, C. M., Heaphy, E. D., Reid, E. M., & Rouse, E. D. (2018). The geography of strain: Organizational resilience as a function of intergroup relations. *Academy of Management Review, 43*(3), 509-529. https://doi.org/10.5465/amr.2016.0004

Kantur, D., & İşeri-Say, A. (2012). Organizational resilience: A conceptual integrative framework. *Journal of Management & Organization, 18*(6), 762-773. doi:10.5172/jmo.2012.18.6.762

Lee, A. V., Vargo, J., & Seville, E. (2013). Developing a tool to measure and compare organizations' resilience. *Natural Hazards Review, 14*(1), 29-41. 10.1061/(ASCE)NH.1527-6996.0000075

Lengnick-Hall, C. A., & Beck, T. E. (2005). Adaptive fit versus robust transformation: How organizations respond to environmental change. *Journal of Management, 31*(5), 738-757. https://doi.org/10.1177/0149206305279367

Lengnick-Hall, C. A., Beck, T. E., & Lengnick-Hall, M. L. (2011). Developing a capacity for organizational resilience through strategic human resource management. *Human Resource Management Review, 21*(3), 243-255. https://doi.org/10.1016/j.hrmr.2010.07.001

Limnios, E. A. M., Mazzarol, T., Ghadouani, A., & Schilizzi, S. G. (2014). The resilience architecture framework: Four organizational archetypes. *European Management Journal, 32*(1), 104-116. 10.1016/j.emj.2012.11.007

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions, 33*(4), 471-476. https://doi.org/10.1007/s10669-013-9485-y

Linnenluecke, M. K., Griffiths, A., & Winn, M. (2012). Extreme weather events and the critical importance of anticipatory adaptation and organizational resilience in responding to impacts. *Business Strategy and the Environment, 21*(1), 17-32. https://doi.org/10.1002/bse.708

Linnenluecke, M. K. (2017). Resilience in business and management research: A review of influential publications and a research agenda. *International Journal of Management Reviews*, *19*(1), 4-30.

Ma, Z., Xiao, L., & Yin, J. (2018). Toward a dynamic model of organizational resilience. *Nankai Business Review International, 9*(3), 246-263. 10.1108/NBRI-07-2017-0041

Mafabi, S., Munene, J., & Ntayi, J. (2012). Knowledge management and organisational resilience: Organisational innovation as a mediator in Uganda parastatals. *Journal of Strategy and Management, 5*(1), 57-80. 10.1108/17554251211200455

Mallak, L. (1998). Putting organizational resilience to work. *Industrial Management, 40*(6), 8-13. https://titusngdotcom.files.wordpress.com/2013/01/putting-organizational-reslience-to-work.pdf

Mallak, L. A. (1998). Measuring resilience in health care provider organizations. *Health Manpower Management, 24*(4-5), 148-52. 10.1108/09552069810215755

Meyer, A. D. (1982). Adapting to environmental jolts. *Administrative Science Quarterly, 27*(4), 515-537. https://doi.org/10.2307/2392528

McManus, S., Seville, E., Brunsden, D., & Vargo, J. (2007). Resilience management: A framework for assessing and improving the resilience of organisations. http://hdl.handle.net/10092/2810

Morgan, S. (2020, November 13). Cybercrime to cost the world $10.5 trillion annually by 2025. *Cybercrime Magazine*. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Onwubiko, C., & Lenaghan, A. P. (2007, May). Managing security threats and vulnerabilities for small to medium enterprises. *IEEE Intelligence and Security Informatics* (pp. 244-249). NJ, USA: IEEE.

Ortiz-de-Mandojana, N., & Bansal, P. (2016). The long-term benefits of organizational resilience through sustainable business practices. *Strategic Management Journal, 37*(8), 1615-1631. https://doi.org/10.1002/smj.2410

Pal, R., Torstensson, H., & Mattila, H. (2014). Antecedents of organizational resilience in economic crises—an empirical study of Swedish textile and clothing SMEs. *International Journal of Production Economics, 147*, 410-428. 10.1016/j.ijpe.2013.02.031

Papaioannou, D., Sutton, A., & Booth, A. (2016). Systematic approaches to a successful literature review. *Systematic approaches to a successful literature review*, 1-336. SAGE.

Parker, H., & Ameen, K. (2018). The role of resilience capabilities in shaping how firms respond to disruptions. *Journal of Business Research, 88*, 535-541. https://doi.org/10.1016/j.jbusres.2017.12.022

Pinheiro, R., Frigotto, M. L., & Young, M. (2022). *Towards resilient organizations and societies: A cross-sectoral and multi-disciplinary perspective.* Bern, Switzerland: Springer Nature. 10.1007/978-3-030-82072-5

Prayag, G., Chowdhury, M., Spector, S., & Orchiston, C. (2018). Organizational resilience and financial performance. *Annals of Tourism Research, 73*, 193-196. 10.1016/j.annals.2018.06.006

Sawalha, I. H. S. (2015). Managing adversity: understanding some dimensions of organizational resilience. *Management Research Review, 38*(4), 346-366.

Schein, E. H. (1985). *Organizational culture and leadership*. USA: John Wiley & Sons.

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*, 154-176.

Somers, S. (2009). Measuring resilience potential: An adaptive strategy for organizational crisis planning. *Journal of Contingencies & Crisis Management, 17*(1), 12–23. https://doi.org/10.1111/j.1468-5973.2009.00558.x

Spagnoletti, P., & Za, S. (2021). Digital resilience to normal accidents in high-reliability organizations. In S. Aier, P. Rohner, & J. Schelp (Eds.), *Engineering the Transformation of the Enterprise: A Design Science Research Perspective* (pp. 339–353). Springer International Publishing. https://doi.org/10.1007/978-3-030-84655-8_21

Vogus, T. J. & Sutcliffe, K. M. (2003). Organizing for resilience. Positive organizational scholarship: Foundations of a new discipline. In K.S. Cameron, J.E. Dutton, & R.E. Quinn (Eds.), *Positive organizational scholarship: Foundations of a new Discipline* (pp. 94-110). San Francisco: Berrett-Koehler Publisher.

Vogus, T. J., & Sutcliffe, K. M. (2007). Organizational resilience: Towards a theory and research agenda. *2007 IEEE International Conference on Systems, Man and Cybernetics*, 3418–3422. https://doi.org/10.1109/ICSMC.2007.4414160

Swanson, M. & Guttman, B. (1996). *Generally accepted principles and practices for securing information technology systems. Gaithersburg*, MD: National Institute of Standards and Technology. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=890092

Taleb, N. N. (2007, April 22). The black swan: The impact of the highly improbable. *The New York Times.* https://www.nytimes.com/2007/04/22/books/chapters/0422-1st-tale.html

Tejay, G., & Klein, G. (2021). Organizational cybersecurity journal editorial introduction. *Organizational Cybersecurity Journal: Practice, Process and People, 1*(1), 1-4. https://doi.org/10.1108/OCJ-09-2021-017

Teo, W. L., Lee, M., & Lim, W. S. (2017). The relational activation of resilience model: How leadership activates resilience in an organizational crisis. *Journal of Contingencies and Crisis Management, 25*(3), 136-147. https://doi.org/10.1111/1468-5973.12179

Van Der Vegt, G. S., Essens, P., Wahlström, M., & George, G. (2015). Managing risk and resilience. *Academy of Management Journal, 58*(4), 971-980. https://doi.org/10.5465/amj.2015.4004

Verizon. (2020). 2020 *Data breach investigations report.* https://www.verizon.com/business/resources/reports/dbir/2020/

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102. http://dx.doi.org/10.1016/j.cose.2013.04.004

Weick, K.E. (1993). The collapse of sensemaking in organizations: The Mann Gulch disaster. *Administrative Science Quarterly*, *38*(4), 628–652. https://doi.org/10.2307/2393339

Weick, K.E. & Sutcliffe, K.M. (2007). *Managing the Unexpected: Assuring high performance in an age of complexity.* San Francisco, CA: Jossey-Bass.

Whitman, Z. R., Kachali, H., Roger, D., Vargo, J., & Seville, E. (2013). Short-form version of the benchmark resilience tool (BRT-53). *Measuring Business Excellence, 17*(3), 3-14. 10.1108/MBE-05-2012-0030

Wood, M. D., Wells, E. M., Rice, G., & Linkov, I. (2019). Quantifying and mapping resilience within large organizations. *Omega*, 87, 117-126. 10.1016/j.omega.2018.08.012

World Economic Forum, (2022). *Global Risk Report*. https://www.weforum.org/reports/global-risks-report-2022/

World Economic Forum, (2023). *Global Risk Report*. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

Youssef, C. M., & Luthans, F. (2007). Positive organizational behavior in the workplace: The impact of hope, optimism, and resilience. *Journal of Management, 33*(5), 774-800. https://doi.org/10.1177/0149206307305562