Received: 23 July 2021 | Revised: 26 January 2022 | Accepted: 23 February 2022

DOI: 10.1002/kpm.1707

SPECIAL ISSUE ARTICLE

WILEY

Knowledge management and knowledge security—Building an integrated framework in the light of COVID-19

Malgorzata Zieba[1] | Ivano Bongiovanni[2]

[1]Faculty of Management and Economics, Department of Management, Gdansk University of Technology, Gdansk, Poland

[2]School of Business, University of Queensland, Brisbane, Australia

Correspondence
Malgorzata Zieba, Faculty of Management and Economics, Department of Management, Gdansk University of Technology, Gdansk, Poland.
Email: mz@zie.pg.gda.pl

Abstract

This paper presents a framework of knowledge risk management in the face of the COVID-19 crisis, derived from the literature on knowledge management, knowledge security, and COVID-19. So far, both researchers and practitioners have focused on knowledge as an asset and their efforts have been aimed at the implementation of knowledge management in various organizational contexts. However, with increasing threats related to cyberattacks or hazards associated with knowledge loss (as magnified by the COVID-19 crisis), there is a growing need to account for knowledge-related risks. In this conceptual paper, we integrate the contributions from the knowledge management and knowledge security fields, together with research on COVID-19 to help organizations protect the knowledge they create, store and share. Based on a structured literature review, our investigation provides researchers and managers with a framework for securely handling organizational knowledge in a critical situation. Our framework revolves around two foci: one the one hand, building appropriate knowledge risk measures and controls; on the other hand, holistically tackling knowledge risks as part of knowledge management activities.

1 | INTRODUCTION

At present, dramatic challenges have risen for public and private organizations alike in how they manage the knowledge they produce, maintain, and exchange (Bratianu, 2020; Bratianu & Bejinaru, 2021; Cegarra-Navarro, Vătămănescu, & Martínez-Martínez, 2021; Cegarra-Navarro, Wensley, et al., 2021). Besides its dramatic consequences on human health (according to the COVID-19 Weekly Epidemiological Update published on 11.01.2022, COVID-19 has caused globally more than 5.4 deaths [*COVID-19 Weekly Epidemiological Update*, 2022]), COVID-19 is having an undeniable economic impact. To prevent the dynamic spread of the disease and the collapse of health care systems, it has been necessary to reduce the economic activity by keeping employees from work and consumers from their purchases (Baldwin & Mauro, 2020, p. 8). This of course has caused serious economic consequences. The United Nations predicted the pandemic will reduce the 2020 world economy by 3.2%, which is the highest figure since the Great Depression (Associated Press (AP), 2020). According to the forecast vintage (December 2020), in advanced economies the median depth of the recession was −7.9%, while in emerging and developing economies the median depth of the recession was −8.8% (Gómez-Pineda, 2020, p. 67). Further, forecasts by the World Economic Forum (2020) show how the pandemic will likely push 40–60 million people into extreme poverty. Finally, according to the World Trade Organization (WTO), in 2020 a significant downturn in global trade was expected, in the range of 13–32%, depending on the development of the situation (e.g., duration of lockdowns) (Bekkers et al., 2020). Undoubtedly, the consequences of the COVID-19 will be serious and long-term and new measures and tools are needed to help organizations overcoming them.

The global pandemic has facilitated the emergence of new practices. An example can be remote working or working from home, which has become a must for a considerable group of workers (Arntz et al., 2020) and brought many challenges, for example, inequality related with household works or occupational segmentation (Kramer & Kramer, 2020). Among other practices, there are virtual connections with customers and providers, and changing working patterns, for example, for example team collaboration (Waizenegger et al., 2020). At the same time, new threats have risen: increased unemployment due to raising redundancies (Blustein et al., 2020; Gallant et al., 2020), decreased levels of trust in the economy (Bunker, 2020; Khurshid, 2020; Lovari, 2020), disrupted supply chains (Aday & Aday, 2020; Ivanov & Das, 2020; Mollenkopf et al., 2020), etc. In these challenging circumstances, businesses, in particular SMEs, which are usually less resilient than large incumbents, have to find new ways to leverage their knowledge and, where possible, protect it from such new threats.

Since the arise of knowledge management field, knowledge has been perceived as a strategic asset and organizations effectively managing it could benefit from an improved market position (Darroch & Mcnaughton, 2003) or, in the best case scenario, achievement of competitive advantage (Lee & Lan, 2011). Other benefits of appropriate KM also included: better operational performance (Andreeva & Kianto, 2012; Darroch, 2005; Vaccaro et al., 2010), improved customer satisfaction (Edvardsson & Durst, 2013; Wei & Wang, 2011), and production of innovation (Du Plessis, 2007; Junges et al., 2015). However, recent research has underlined the possibility for significant *downsides* connected with knowledge, namely the detrimental effects associated with its loss, its capture by competitors or its waste, defined as 'not making use of available and potentially useful knowledge in the organization' (Durst & Zieba, 2019, p. 5). This has led to the development of nascent literature on knowledge risks (Bratianu, 2018; Durst et al., 2016; Durst & Zieba, 2019; Zieba & Durst, 2018). As a new area of study, knowledge risks have not been examined extensively so far and therefore, there is no clear guidance on how organizations should be handling them, especially now, in the face of the COVID-19 pandemics. In these new settings, KM and knowledge security systems appear to be possibly useful tools for organizations in handling for example, fact disinformation and ensuing over-, or inadequate reactions, lack of reliable knowledge sources, lack of skills for crisis detection and response, increase in information asymmetry, exploitation of general uncertainty by cyber-criminals (e.g., increase in cyber-frauds; Interpol, 2020), etc.

What benefits could KM and knowledge security mechanisms produce in the light of the COVID-19 crisis? We believe three orders of benefits exist. First, **the changing competitive scenario requires companies to better utilize knowledge** they collect, store, elaborate, and share to produce competitive advantage. Second, **knowledge supports the usage of vital resources in times of crisis** (for example, the best allocation of shrinking budgets, the deployment of staff to crucial functional areas or the most effective ways to communicate the crisis externally). Third, **organizations that demonstrate superior utilization and protection of knowledge can rebuild trust in customers and other stakeholders**, which has the potential to create competitive advantage in times where trust is fast depleting. We offer here a framework to integrate knowledge security as a fundamental organizational activity, an inseparable part of a KM approach, for organizations operating under the challenging circumstances of the global pandemic. Despite an acknowledgement of their importance in the face of crises, research and practice in KM and security are still in their infancy (Ahmad et al., 2014; Manhart & Thalmann, 2015; Obitade, 2019). In particular, KM researchers do not seem to pay sufficient attention to knowledge security, considering it more like a subcomponent of a broader KM system (Jennex & Zyngier, 2007). By means of our conceptual framework, we aim at supporting organisations at the mercy of the COVID-19 crisis in better managing and protecting their knowledge. After a concise literature review, we illustrate our methodology. Then we elaborate on our results and discussion and finally, we conclude the paper.

2 | KNOWLEDGE MANAGEMENT AND KNOWLEDGE MANAGEMENT MODELS

A variety of models and approaches to KM are present in the literature. For example, Bukowitz and Williams (2000, p. 8) developed a KM process framework which aims at helping organizations in generating, keeping, and deploying strategically valid knowledge for value creation. At its core, this cyclical model entails an exchange of knowledge between the organization and the external world, where learning mechanisms derive from knowledge usage and continuous knowledge assessment allows organizations to sustain their KM efforts. Knowledge in this framework may consist of knowledge repositories, information technologies, communications infrastructures, process know-how, external resources, etc. (Dalkir, 2011). Probst et al. (2000) have proposed a KM framework composed by the following organizational processes: *knowledge localization*; *knowledge acquiring* (either from inside the organization or its environment); *knowledge development*; *knowledge sharing and dissemination*; *knowledge usage*; and *knowledge retaining* (consisting of three stages: choosing knowledge residing in people, events, or processes that is worth preserving, preparing this knowledge for storage, and updating organizational knowledge). Similarly, Alavi and Leidner (2001) have offered a process-based framework in which organizations are involved in four knowledge processes, namely: knowledge creation, knowledge storage/retrieval (organizational memory, where knowledge is kept in different forms and formats), knowledge transfer (which can happen between individuals in the organization, from individuals to other sources, from individuals to groups, among groups or from a group to the overall organization) and knowledge application (the utilization of knowledge for the purpose of creating value and organizational competitive advantage). Finally, Chan and Chao (2008) have proposed a unified KM model in which knowledge is acquired, protected, applied and converted into value, with the support of specific infrastructural capabilities, namely technology, structure and culture.

Processes associated with knowledge can therefore be summarized as follows: (1) Acquiring knowledge from internal and external sources; (2) Searching for, and localizing, organizational knowledge to be managed; (3) Developing and converting knowledge into value; (4) Sharing and disseminating knowledge within the organization and between the organization and the environment (e.g., clients, collaborators, etc.); (5) Using and applying knowledge in the required settings; and (6) Retaining and sustaining knowledge. In addition, KM processes need to be led by previously established knowledge goals, a step that is preliminary to the ones here identified (Probst et al., 2000).

In the face of a crisis like COVID-19, knowledge-related processes should be faster and more accurate. On the one hand, the crisis requires companies to quickly acquire knowledge from external sources (e.g., to be kept up-to-date about recent developments in the market) or develop/convert existing knowledge into value; on the other hand, it is crucial to carefully sift accurate knowledge from unreliable one, which seems to abound in times of crises (Pennycook et al., 2020; Renkel et al., 2020; van Bavel et al., 2020). One also needs to consider the potential negative consequences related to counter-knowledge, which can be defined as "sources of unverified information, gossip, partial truths, or deliberate lies, which can be in certain contexts mistaken for true facts" (Bolisani et al., 2021, p. 517). According to the study by Cegarra-Navarro, Vătămănescu, and Martínez-Martínez (2021), Cegarra-Navarro, Wensley, et al., 2021), counter-knowledge may lead to evasive knowledge hiding, and further to defensive reasoning. If it is continues in a vicious cycle, it may result in bad decision making and lead to distrust in public institutions (Cegarra-Navarro, Bolisani, & Cepeda-Carrión, 2021). This is especially valid in a crisis situation, such as COVID-19 pandemic. At the same time, some established knowledge processes may have become ineffective. For example, informal organizational meetings may need to be replaced with virtual ones. Also retaining and sustaining knowledge may constitute a challenge when employees are made redundant. Another challenge related to this new situation is potential knowledge hiding due to defensive routines people might develop. In a study by Cegarra-Navarro, Vătămănescu, and Martínez-Martínez (2021), Cegarra-Navarro, Wensley, et al., 2021), it has been proved that unlearning does not just influences defensive reasoning but also indirectly has an impact on knowledge hiding. These are new challenges organizations must become aware of.

All the knowledge processes revised or implemented from scratch in an organization in the face of COVID-19, in order to be consolidated and accepted by employees, need to be integrated within the organizational fabric, namely organizational culture, structure and technology. Organizations often concentrate only on the technological aspects of KM processes, for example implementing a KM technology solution and neglecting culture and structures necessary to accompany such change. Moreover, organizations might find it difficult to focus on the latter aspects in the new conditions set by the crisis (e.g., due to lack of time and resources, new challenges of emerging working practices, etc.).

In order to unpack the connections that link KM and its processual models with knowledge security, we will now briefly review relevant literature on the latter.

2.1 | Knowledge security

Sitting at the intersection between KM and information security (Desouza, 2006), knowledge security is defined by Ilvonen (2013, p. 152) as '…the process of making and keeping the knowledge of people working at a company secure'. According to Bose (2003, p. 70), knowledge security can be defined as 'the measures taken to protect knowledge from accidental or intentional disclosure to unauthorized persons and from unauthorized alteration'. In this definition, the significance of knowledge is highlighted based on the risks associated with its disclosure or alteration; external threats are indicated; and the basic components of a risk management approach to knowledge security are laid.

In the light of the COVID-19 crisis, companies need to account for emerging dynamics in order to secure their knowledge. Ilvonen's definition stems from the very ontology of the concept of *security*, as deriving from Latin *secare* (to saw), meaning separating something (of value) from something else (a threat). Global crises like COVID-19 invite us to reconsider the *loci* of our life, in this case, work. *Where does the separation of what is valuable (knowledge) from the threat (the external world) happen*? The emergence of practices such as remote or smart working, reliance on cloud computing or the storage of data and information on private devices makes such separation (*security*) a more challenging task. Organizational boundaries are progressively less effective in ensuring the protection of knowledge, since the current crisis has made organizations more *asymmetric*. Furthermore, traditionally public and private organizations rely on fragmented initiatives to increase their protection (e.g., knowledge leakage). Even when present, such initiatives are drawn from an information security standpoint, which, alone, is often too technical and too difficult to grasp by employees and board of directors alike (Ahmad et al., 2014).

Knowledge security has three dimensions: people, products, and processes (Desouza, 2006). Along these dimensions, several implications can be extracted. First, when the dimension of people is concerned, it can be useful to mix hard and soft measures from information security (e.g., firewalls and employee training). In times of COVID-19, this holds particularly true, as organizations rely on employees working from remote to put in place appropriate practices (e.g., using authorized software on work devices, connecting through Virtual Private Networks, etc.). Second, when products are considered, it might be useful to draw lessons from information security management as well (e.g., the explicit form of knowledge in the form of documents may be protected with confidentiality clauses or security tagging). Smart working practices require digitalisation of such measures. Third, with regard to processes, procedures for knowledge communication, especially in the case of relationships with externals, need to be established. As an example, governments that have invited their citizens to utilize contagion mapping devices in the wake of COVID-19 have promptly responded to users' questions around privacy and security (Australian Government, 2020; Government of Singapore, 2020).

As a complement to these components, and an expansion of the product dimension, Ross and Schulte (2005) suggest that knowledge security should be provided with appropriate technologies for KM. Examples of these technologies can be secure networks, password-protected platforms, multi-factor authentication, etc. A delicate balance exists in these situations: too much access to knowledge, and employees can potentially endanger it; not enough access to knowledge, and the creation of value from knowledge sharing can be hampered. A balance between knowledge sharing and knowledge protection is paramount in a sound knowledge risk management system (Manhart & Thalmann, 2015). Besides the aforementioned structural implications for knowledge security, COVID-19 has also the potential to produce indirect implications: an example could be a disgruntled, redundant employee that willingly tampers with organizational knowledge in retaliation. In the next section, we will describe the method adopted in our research. Our aim is to propose a knowledge risk management framework for organizations to identify and overcome their knowledge threats in the wake of COVID-19.

3 | METHODOLOGY

This paper uses structured literature review to analyze three areas: KM, knowledge security, and the COVID-19 crisis. The output is a framework for knowledge risk management in the wake of the COVID-19 crisis. To perform the analysis, we followed the three-step procedure proposed by Manhart and Thalmann (2015), that is, first we identified the relevant literature; second we structured the review; and finally, we proposed the contribution to the theory in the form of the framework for knowledge risk management.

To provide the framework, we first applied the author-centric approach, where we prepared a review of particular publications with regard to the concepts discussed by the author(s), as proposed by Webster and Watson (2002), namely Author A … concept X, concept Y,…. After analyzing particular publications with regard to the concepts they discussed, we transformed the results into concept-centric, extracting the main outcomes concerning knowledge management and knowledge security. Along the process, we kept in mind the recommendation of Webster and Watson (2002), who stated that 'a review succeeds when it helps other scholars to make sense of the accumulated knowledge on a topic' (p. xvii). We have provided the following elements of the reviewed literature for this purpose: description, theoretical implications, practical contributions, main contribution for the present paper and synthetic attribution. Table 1 offers a detailed overview of the articles and sources investigated in our review.

The resulting framework is presented in the next section.

4 | RESULTS AND DISCUSSION

Our framework is based on components singled out in the aforementioned pieces of research, in particular in Desouza (2006), Ross and Schulte (2005), and (Manhart & Thalmann, 2015) and adapted to cater for the dynamics of the COVID-19 crisis. We illustrate it based on two *foci*: first, the risk management controls; and second, the risk management process.

As with any knowledge risk management system, our model aims at mitigating the consequences, or reducing the likelihood, of knowledge risks in an organizational setting facing a crisis (e.g., COVID-19). Controls and measures are therefore built around knowledge risks, and stem from three types of mechanisms (legal, organizational, and technical) and have three targets (people, processes, and products) (Figure 1). In each specific target, sub-components can be derived as follows: as for people, training and awareness can be improved by 'borrowing' methods from information security management and focusing on the development of soft skills for knowledge risk management; in terms of products, 'hard skills' can be complemented by deploying adequate information security technologies; and finally, in terms of processes, sound stakeholder and communication management capabilities need to be developed. As far as the mechanisms are concerned, they are of three types: legal, organizational and technical. Legal mechanisms concern laws and regulations available at different levels (e.g., national, international, union) that can help organizations in protecting themselves against knowledge risks, for example, industrial espionage, security breaches or intellectual property theft. Organizational mechanisms concern all types of actions that may be undertaken by various organizational members to mitigate knowledge risks, for example, creation of knowledge sharing culture, implementation of KM initiatives and practices, creation of knowledge maps, undertaking knowledge risks measures (e.g., identifying knowledge at risk and proposing ways of eliminating it). Finally, technical mechanisms are related to all types of technologies and technical solutions that may help organizations in controlling knowledge risks. Those can be tools for knowledge storage and sharing, collaborative tools, antivarious software, verification procedures to limit the access of unauthorized people to knowledge, etc. In general, tools helping in the provision of knowledge security are very useful here. All those mechanisms can concern one or more of three targets, namely people, processes, and products.

Knowledge risk controls alone are not sufficient in the COVID-19 crisis to ensure the security of organizational knowledge and adequate processes for risk management are necessary. Based on our review of the literature, we have singled out the following ones, which built a connection between KM and knowledge security, as a component of the former. From acquisition of knowledge from external and internal sources, to retention and maintenance of knowledge, the steps in this process should not be conceived in a chronological, mono-directional order, but as the phases of a KM process in which knowledge security is integrated with specific activities, and integrated within the organizational culture, technology and structure (Figure 2). It has to be taken into account that COVID-19 pandemic has changed the functioning of organizations, as indicated in the introduction of this paper, and the proposed framework integrates those changes (they are marked in red color in the figure). First of all, organizations due to problems with selling their products in the pandemic (e.g., megastores, clothing industry, etc.) cannot count on their revenues to the same extent as previously and therefore, they often need to make reductions in investments and they have limited resources (e.g., they might need to fire some employees or limit their operational scale). Managing knowledge is more challenging in such conditions (e.g., organizations might lose some of its knowledge due to reductions in employment). When organizations undertake their knowledge security actions, they also need to address some challenges related to the pandemic. For example, in the face of disinformation and counter-knowledge creation, there is a risk of obtaining unreliable knowledge

TABLE 1

Paper/source title	Authors, (year)	Description	Theoretical implications	Practical contributions	Main contribution for the present paper (and *synthetic attribution*, see Figure 1 and Figure 2)
Managing knowledge: Building blocks for success	Probst, G., Romhardt, K., & Raub, S. (2000)	A KM framework composed of several organisational processes	The building blocks for the re-design of any KM framework are offered and articulated in a composite way, laying the foundations for a reflection on how an innovative KM framework could look like to address COVID-19's challenges.	Practitioners in KM are warned to identify appropriate KM goals before designing their KM framework.	Offered the essential steps for the re-design of KM processes under COVID19 constraints: acquiring knowledge, searching for and localising knowledge, development and conversion of knowledge, sharing and dissemination of knowledge, usage and application of knowledge, and retaining and sustaining knowledge (*Re-design of KM processes*) Emphasised the relevance of preliminary establishment of knowledge goals, prior to establishing any knowledge risk management framework (*Knowledge goals*)
Knowledge management in small and medium-sized enterprises	Chan, I., & Chao, C.-K. (2008)	A unified KM model in which knowledge is acquired, protected, applied, and converted into value	In the face of the uncertainties that they typically face, SMEs need to increase the resources they utilise to harness the value of knowledge effectively. Knowledge management capability is determined by a balanced combination of structure, culture, and technology.	(1) Companies are encouraged to set up appropriate plans for the acquisition of knowledge (2) Management can facilitate the conversion of individual knowledge in a collective resource (3) Employees should be offered opportunities to experiment with their knowledge (4) Management should be in charge with setting up plans to protect knowledge	Contributed specific infrastructural capabilities that serve to integrate KM in the organisational fabric: culture, technology, and structure (*Integration of KM with organisational culture, technology, and structure*)
Security as a contributor to knowledge management success	Jennex, M. E., & Zyngier, S. (2007)	A KM success model is proposed to illustrate how security (in particular, risk management) and associated models (e.g., the National	The article identifies bodies that are responsible for governance activities within the proposed KM framework, their roles, and their tasks.	The article incorporates knowledge security into KM practices.	Contributed a focus on incorporating a knowledge security component in the proposed knowledge risk management

(Continues)

TABLE 1 (Continued)

Paper/source title	Authors, (year)	Description	Theoretical implications	Practical contributions	Main contribution for the present paper (and *synthetic attribution*, see Figure 1 and Figure 2)
		Security Telecommunications and Information System Security Committee [NSTISSC] security model) can be applied to KM management support and governance and KM strategic activities	The article also identifies and analyses the fundamental processes that govern KM. The research contributes an operationalizable framework for organisations to leverage authority, risk-management, financial control, and measurement for KM purposes.		framework (*Knowledge security*)
Knowledge Management and Knowledge Systems: Conceptual Foundations and Research Issue	Alavi, M., & Leidner, D. E. (2001)	An extensive review of KM literatures with the purpose of identifying prominent areas for future research in this field	This review examines KM literatures in different fields and highlights the most important areas for future research.	A process view of organisational knowledge management with a deep-dive in the role of IT to support it.	Contributed a process-based approach to KM (*process-based approach of the proposed knowledge risk management framework*)
Using social and behavioural science to support COVID-19 pandemic response	van Bavel, J.J., Baicker, K., Boggio, P.S., Capraro, V., Cichocka, A., Cikara, M., Crockett, M.J., et al. (2020)	A discussion of extensive evidence on pandemics-related research topics such work on navigating threats, social and cultural influences on behaviour, science communication, moral decision-making, leadership, and stress and coping, with emphasis on practical insights for effective response to the COVID-19 pandemic and on outstanding research gaps	The paper reviews historical work on issues related to pandemics in the social and behavioural: threat perception, social context, science communication, aligning individual and collective interests, leadership, and stress and coping.	Behavioural and social sciences can offer support in mitigating the potentially devastating effects of COVID-19, in particular around health communication strategies.	Offered an understanding of the dynamics that characterise the distinction between accurate and unreliable sources of knowledge and the latter's abundance in times of crisis (*Unreliable knowledge*)
Fighting COVID-19 misinformation on social media: Experimental evidence for a scalable accuracy nudge intervention	Pennycook, G., McPhetres, J., Zhang, Y. and Rand, D.G. (2020)	A study that unpacks the reasons why individuals share false information on COVID-19 on social media. The study demonstrates that nudging people to think about accuracy improves choices about what to share on social media.	This study confirms the existence of an inattention-based account of COVID-19- misinformation transmission on social media, whereby accuracy of the shared information is low due to users' low attention to the contents they share	Nudging users and prompting them to pay more attention on the accuracy of the information about COVID-19 shared on social media can help reduce the extent of disinformation about the pandemic.	Offered an understanding of the reasons why individuals share unreliable information about COVID-19 on social media and suggested nudging as a simple strategy to counter this (*Unreliable knowledge*)
Knowledge management-enabled health care	Bose, R. (2003)	This study conceptualises a knowledge	This research confirms the growing realisation that a	This study offers managers in healthcare a	Provides the definition of Knowledge Security utilised in

TABLE 1 (Continued)

Paper/source title	Authors, (year)	Description	Theoretical implications	Practical contributions	Main contribution for the present paper (and *synthetic attribution*, see Figure 1 and Figure 2)
management systems: Capabilities, infrastructure, and decision-support		management-enabled healthcare management system to integrate clinical, administrative, and financial processes in health care and through a common technical architecture. The study also contributes a decision support infrastructure for clinical and administrative decision-making.	more diffused use of appropriate IT could increase efficiency of, and improve the performance of, healthcare decision-making systems in the industry, together with protecting the confidentiality of patient information.	management system (backed with the appropriate IT infrastructure) to support decision-making by integrating clinical, administrative, and financial processes in healthcare.	the proposed framework (*the measures taken to protect knowledge from accidental or intentional disclosure to unauthorised persons and from unauthorised alteration)*
Protecting organisational competitive advantage: A knowledge leakage perspective	Ahmad, A., Bosua, R., & Scheepers, R. (2014)	A conceptual framework to protect organisational knowledge and preserve competitive advantage, with specific focus on knowledge leakage.	This article synthesises the measures to protect knowledge and information in organisations across four categories: Strategic-Level Management Initiatives, Operational-Level Knowledge Protection Processes, Supporting Technology Infrastructure, and Legal Structures	The article emphasises the need for a more comprehensive managerial framework to enable organisations to calibrate their current approaches and manage information and knowledge protection more strategically.	Warns against the exclusive utilisation of technical information security measures as the sole way to protect knowledge from leakage
Knowledge Security: An Interesting Research Space	Desouza, K. (2006)	A foundational, conceptual article that paves the way towards investigation knowledge security and its composing dimensions.	Operating at the intersection between KM and information security, knowledge security is an under-explored area that yet can secure competitive advantage to organisations.	Organisations need to pay attention to the three levels in which knowledge security can be ensured: products, people, and processes	Offers the targets of knowledge risk management controls proposed in our framework: *people, products, and processes*. Emphasised the importance of setting appropriate knowledge security controls and measures in any proposed framework (*determination of knowledge security controls and measures*)
Protecting organisational knowledge: a structured literature review	Manhart, M., & Thalmann, S. (2015)	A comprehensive review of the literature on the protection of organisational knowledge, with	The paper highlights how the concept of tacit knowledge is an under-investigated one. The same applies to knowledge	This study offers an exhaustive overview of current knowledge protection practices from the literature.	Contributes the three-step process which we utilised as our research methodology to

(Continues)

TABLE 1 (Continued)

Paper/source title	Authors, (year)	Description	Theoretical implications	Practical contributions	Main contribution for the present paper (and *synthetic attribution*, see Figure 1 and Figure 2)
		focus on establishing research gaps and areas for further investigation.	protection phenomena and to associated frameworks, which need to be further developed and tested.		elaborate our framework Contributes the tripartite dimension of legal-organisational-technical for existing mechanisms for knowledge protection (*legal-organisational-technical*)

and make wrong decisions on its basis. Knowledge goals that organizations might have set in the past, might need to be shifted into new ones. Also investing in knowledge security controls and measures might appear a challenge due to reduction in investments. Moreover, the integration of KM with organizational culture, technology, and structure can be pressed by COVID-19 due to redundancies and systemic changes (e.g., organizational culture of knowledge sharing might be hindered by the risk of job loss or customers might switch to other products, e.g. more sustainable). The proposed framework illustrates the potential integration of knowledge management with knowledge security in the light of COVID-19 pressures. It is presented in the figure below.

To sum up, the framework presents the connections existing between KM and knowledge security, together with the potential pressures exerted by COVID-19. The identification of those pressures is important, as it makes the implementation of the framework more challenging. If in the face of a crisis an organization wants to implement a knowledge security initiative as part of its existing KM efforts, it needs to start with the identification of valuable knowledge. This knowledge has to be managed and secured in the first step. When this knowledge is identified, knowledge goals have to be established, for example, what the organization aims to do with the knowledge and how it aims to handle it, keeping in mind for example the threats resulting from virtual work and the dynamically changing situation. The third step is the determination of knowledge security measures suitable for the crisis situation. This step is crucial, as it establishes how knowledge requirements can be protected, considering the threats and risks related to this knowledge and the special environmental conditions. At this stage, organizations need to carefully consider potential knowledge risks they are endangered with. Only after this step, KM processes can be designed, with a special emphasis placed on knowledge security throughout all of them. Without the basic assumptions concerning knowledge security, it would be risky to handle valuable knowledge by any organization, especially in a crisis like COVID-19. When KM processes are designed, they can be implemented by the integration with organizational culture, technology and structure. For example, valuable knowledge has been identified as a piece of technological intellectual property (TIC) worth protection in an organization. The knowledge goal will be to protect this TIC from the external threats (e.g., a hacker attack), as well as internal risks (e.g., knowledge espionage), making this TIC available for the benefit of the organization. Knowledge security controls and measures could be for instance the legal agreements with employees having access to this TIC: such agreements could establish the consequences arising in case of release of TIC to external parties; the limitations imposed onto access to TIC; a categorization of trusted vs untrusted users; adequate security measures for smart-working practices; etc. When KM processes are designed, TIC should be considered with care and excluded from some processes, for instance from sharing and dissemination via unprotected networks.

5 | CONCLUSION

The knowledge risk management framework for the COVID-19 crisis presented in this conceptual paper is derived from a review of selected literature in KM, knowledge security, and COVID-19. Our research casts light on the relationship between KM and knowledge security and lays the foundations for the systematic addressing of knowledge issues in modern organizations as potentially subject to specific risks (e.g., knowledge theft or loss) that need targeted interventions. Such interventions are built around two *foci*: one the one hand, building appropriate knowledge risk measures and controls; on the other hand, holistically tackling knowledge risks as part of the KM activities. One needs to remember that knowledge risk management is a new field of study and as such, it does not offer full understanding and there is a place for future development. In addition, new areas of knowledge risk management are being covered all the time and examined in the latest studies, for example, counter-knowledge and its potential negative impact in the face of COVID-19 crisis (Bolisani et al., 2021). Our paper contributes to the ongoing, nascent research on the COVID-19 crisis and offers systemic support for organizations

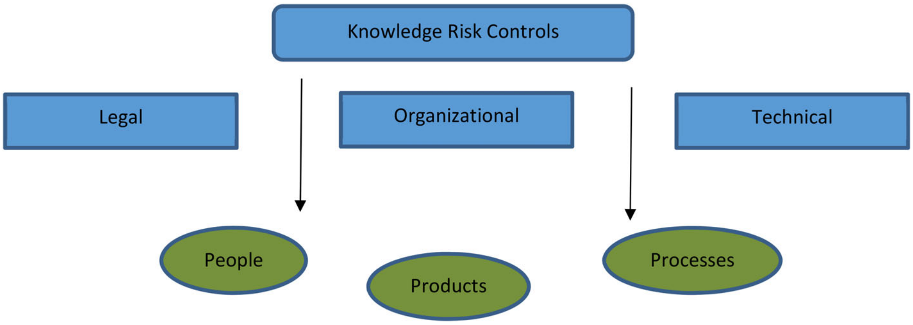

FIGURE 1 Knowledge risk measures and controls: Types and targets [Colour figure can be viewed at wileyonlinelibrary.com]

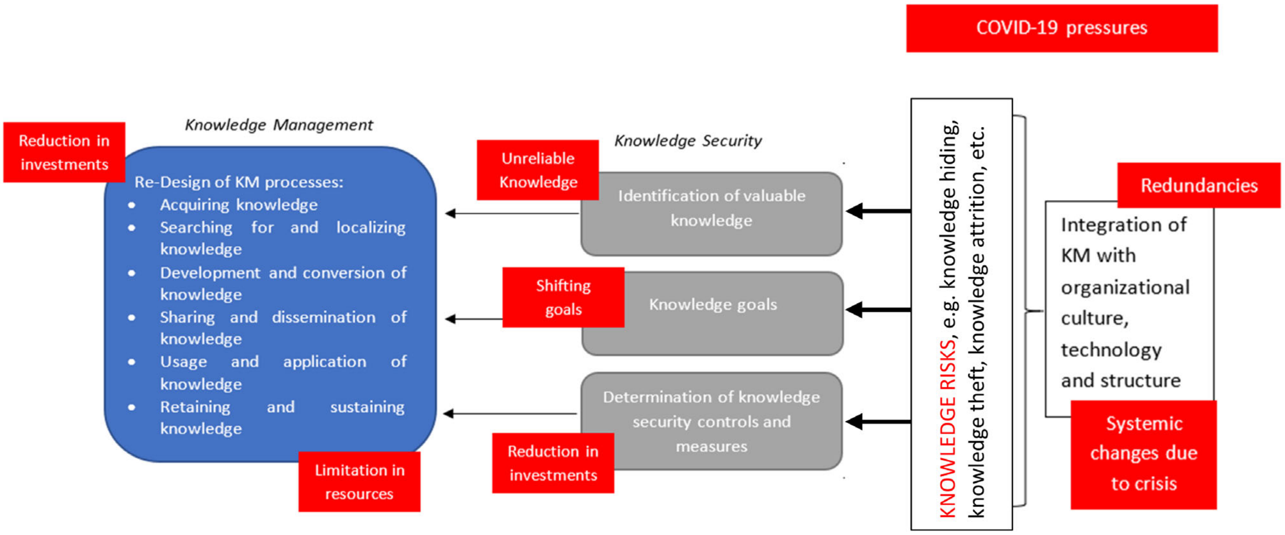
COVID-19 pressures
Knowledge Management
Reduction in investments
Re-Design of KM processes:
Acquiring knowledge
Searching for and localizing knowledge
Development and conversion of knowledge
Sharing and dissemination of knowledge
Usage and application of knowledge
Retaining and sustaining knowledge
Limitation in resources
Knowledge Security
Unreliable Knowledge
Identification of valuable knowledge
Shifting goals
Knowledge goals
Determination of knowledge security controls and measures
Reduction in investments
KNOWLEDGE RISKS, e.g. knowledge hiding, knowledge theft, knowledge attrition, etc.
Redundancies
Integration of KM with organizational culture, technology and structure
Systemic changes due to crisis

FIGURE 2 Knowledge risk management framework with pressures exerted by the COVID-19 crisis [Colour figure can be viewed at wileyonlinelibrary.com]

facing it. It also offers organizations a tool for analyzing their knowledge management approach in relation to the provision of the knowledge security and management of knowledge risks. Linking these three concepts is novel and at the same time necessary, as it allows to achieve a synergy effect in a better way of handling the COVID-19 crisis. At the same time, KM research can achieve a new level of exploration by the examination of its link with other, related fields and disciplines (e.g., knowledge security).

There are several limitations that affect this paper. First, our framework is of a conceptual character and needs to be empirically tested. Second, our investigation is not based on a systematic (i.e., holistic) literature review, which could have expanded the scope and generalizability of our research. Third, the COVID-19 crisis is an under-explored phenomenon whose social, health-related, and economic impact is yet to be fully seized and therefore, this study should be treated as a preliminary one, not presenting the long-term consequences of the COVID-19 pandemic.

As a result, we invite fellow researchers to join us in exploring the following directions. First, our knowledge risk management model can be tested in a variety of organizations from different sectors, settings and countries, to test its applicability and usefulness in times of crisis. Second, a systematic literature review can be conducted to elaborate an alternative or more complete model, for example by combining sub-components of KM and knowledge security systems. In this sense, investigations in the literature have already proposed promising avenues, such as the intersection between cybersecurity management and intellectual capital (Renaud et al., 2019) or between intellectual capital and knowledge security (Bongiovanni et al., 2020). Finally, a quantitative study may follow to examine the perceptions of knowledge security in the COVID-19 crisis among managers of various public and private organizations.

ACKNOWLEDGMENT

Study supported with the research grant received by Malgorzata Zieba from the National Science Centre (Poland) in the context of a research project “Knowledge risks in modern organizations” (No. 2019/33/B/HS4/02250).

DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

ORCID

Malgorzata Zieba https://orcid.org/0000-0002-5138-9330

REFERENCES

Aday, S., & Aday, M. S. (2020). *Impact of COVID-19 on the food supply chain* (pp. 167–180). Food Quality and Safety. https://doi.org/10.1093/fqsafe/fyaa024

Ahmad, A., Bosua, R., & Scheepers, R. (2014). Protecting organizational competitive advantage: A knowledge leakage perspective. *Computers and Security*, *42*, 27–39. https://doi.org/10.1016/j.cose.2014.01.001

Alavi, M., & Leidner, D. E. (2001). Review: Knowledge management and knowledge management systems: Conceptual foundations and research issues. *MIS Quarterly*, *25*(1), 107–136.

Andreeva, T., & Kianto, A. (2012). Does knowledge management really matter? Linking knowledge management practices, competitiveness and economic performance. *Journal of Knowledge Management*, *16*(4), 617–636. https://doi.org/10.1108/13673271211246185

Arntz, M., Ben Yahmed, S., & Berlingieri, F. (2020). Working from home and COVID-19: The chances and risks for gender gaps. *Intereconomics*, *55*(6), 381–386. https://doi.org/10.1007/s10272-020-0938-5

Associated Press, WHO warns virus 'may never go away' as new clusters emerge, https://www.9news.com.au/world/coronavirus-world-updates-un-says-global-economy-to-shrink-who-says-covid-19-here-to-stay/d96473ca-d451-4c83-aad0-fd7130b4363f, date of access: 14.05.2020.

Australian Government (2020), https://www.health.gov.au/using-our-websites/privacy/privacy-policy-for-covidsafe-app, date of access: 18.05.2020.

Baldwin, R., & Mauro, B. W. (2020). Mitigating the COVID economic crisis: Act fast and do whatever it takes. In Ewi-Vlaanderen.Be (issue July). https://voxeu.org/content/mitigating-covid-economic-crisis-act-fast-and-do-whatever-it-takes

Bekkers, E., Keck, A., Koopman, R., Nee, C., Trade and COVID-19: The WTO's 2020 and 2021 trade forecast, 2020, https://voxeu.org/article/trade-and-covid-19-wto-s-2020-and-2021-trade-forecast, date of access: 18.05.2020.

Blustein, D. L., Duffy, R., Ferreira, J. A., Cohen-Scali, V., Cinamon, R. G., & Allan, B. A. (2020). Unemployment in the time of COVID-19: A research agenda. *Journal of Vocational Behavior*, *119*(May), 1–4. https://doi.org/10.1016/j.jvb.2020.103436

Bolisani, E., Cegarra Navarro, J. G., & Garcia-Perez, A. (2021). Managing counter-knowledge in the context of a pandemic: Challenges for scientific institutions and policymakers. *Knowledge Management Research and Practice*, *19*(4), 517–524.

Bongiovanni, I., Renaud, K., & Cairns, G. (2020). Securing intellectual capital: An exploratory study in Australian Universities. *Journal of Intellectual Capital*, *21*(3), 481–505. https://doi.org/10.1108/JIC-08-2019-0197

Bose, R. (2003). Knowledge management-enabled health care management systems: Capabilities, infrastructure, and decision-support. *Expert Systems with Applications*, *24*(1), 59–71. https://doi.org/10.1016/S0957-4174(02)00083-0

Bratianu, C. (2018). A holistic approach to knowledge risk. *Management Dynamics in the Knowledge Economy*, *6*(4), 593–607. https://doi.org/10.25019/MDKE/6.4.06

Bratianu, C. (2020). Toward understanding the complexity of the COVID-19 crisis: A grounded theory approach. *Management and Marketing*, *15*(s1), 410–423. https://doi.org/10.2478/mmcks-2020-0024

Bratianu, C., & Bejinaru, R. (2021). COVID-19 induced emergent knowledge strategies. *Knowledge and Process Management*, *28*(1), 11–17. https://doi.org/10.1002/kpm.1656

Bukowitz, W. R., & Williams, R. L. (2000). *The knowledge management fieldbook*. Financial Times/Prentice Hall.

Bunker, D. (2020). Who do you trust? The digital destruction of shared situational awareness and the COVID-19 infodemic. *International Journal of Information Management*, *55*(July), 102201. https://doi.org/10.1016/j.ijinfomgt.2020.102201

Cegarra-Navarro, J. G., Bolisani, E., & Cepeda-Carrión, G. (2021). Linking good counter-knowledge with bad counter knowledge: The impact of evasive knowledge hiding and defensive reasoning. *Journal of Knowledge Management*. https://doi.org/10.1108/JKM-05-2021-0395

Cegarra-Navarro, J. G., Vătămănescu, E. M., & Martínez-Martínez, A. (2021). A context-driven approach on coping with COVID-19: From hiding knowledge toward citizen engagement. *Knowledge and Process Management*, *28*(2), 134–140. https://doi.org/10.1002/kpm.1662

Cegarra-Navarro, J. G., Wensley, A., Batistic, S., Evans, M., & Para, C. C. (2021). Minimizing the effects of defensive routines on knowledge hiding though unlearning. *Journal of Business Research*, *137*, 58–68.

Chan, I., & Chao, C.-K. (2008). Knowledge management in small and medium-sized enterprises. *Communications of the ACM*, *51*(4), 83–88.

Dalkir, K. (2011). *Knowledge management in theory and practice*. MIT press.

Darroch, J. (2005). Knowledge management, innovation and firm performance. *Journal of Knowledge Management*, *9*(3), 101–115. https://doi.org/10.1108/13673270510602809

Darroch, J., & Mcnaughton, R. (2003). Beyond market orientation knowledge management and the innovativeness of New Zealand firms. *European Journal of Marketing*, *37*(3/4), 572–593. https://doi.org/10.1108/03090560310459096

Desouza, K. C. (2006). Knowledge security: An interesting research space. *Journal of Information Science & Technology*, *3*(1), 1–7.

Du Plessis, M. (2007). The role of knowledge management in innovation. *Journal of Knowledge Management*, *11*(4), 20–29.

Durst, S., Bruns, G., & Henschel, T. (2016). The management of knowledge risks: What do we really know? *International Journal of Knowledge and Systems Science (IJKSS)*, *7*(3), 19–29.

Durst, S., & Zieba, M. (2019). Mapping knowledge risks: towards a better understanding of knowledge management management. *Knowledge Management Research & Practice*, *17*(1), 1–13. https://doi.org/10.1080/14778238.2018.1538603

Edvardsson, I. R., & Durst, S. (2013). The benefits of knowledge management in small and medium-sized enterprises. *Procedia - Social and Behavioral Sciences*, *81*, 351–354. https://doi.org/10.1016/j.sbspro.2013.06.441

Gallant, J., Kroft, K., Lange, F., Notowidigdo, M. (2020). Temporary unemployment and labor market dynamics during the COVID-19 recession. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3702514, date of access: 12.03.2021.

Gómez-Pineda, J. G. (2020). Growth forecasts and the Covid-19 recession they convey. *Covid Economics*, *40*, 196–213.

Ilvonen, I. (2013). *Knowledge security – A conceptual analysis*. PhD Thesis. Tampere University.

Interpol (2020). Cyberthreats are constantly evolving in order to take advantage of online behaviour and trends. The COVID-19 outbreak is no exception, https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats, date of access: 20.05.2020.

Ivanov, D., & Das, A. (2020). Coronavirus (COVID-19 / SARS-CoV-2) and supply chain resilience: A research note. *International Journal of Integrated Supply Management*, *13*(1), 90–102.

Jennex, M. E., & Zyngier, S. (2007). Security as a contributor to knowledge management success. *Information Systems Frontiers*, *9*(5), 493–504. https://doi.org/10.1007/s10796-007-9053-4

Junges, F. M., Gonçalo, C. R., Garrido, I. L., & Fiates, G. G. S. (2015). Knowledge management, innovation competency and organisational performance: A study of knowledge-intensive organisations in the IT industry. *International Journal of Innovation and Learning*, *18*(2), 198–221. https://doi.org/10.1504/IJIL.2015.070867

Khurshid, A. (2020). Applying Blockchain technology to address the crisis of trust during the COVID-19 pandemic. *JMIR Medical Informatics*, *8*(9), e20477. https://doi.org/10.2196/20477

Kramer, A., & Kramer, K. Z. (2020). The potential impact of the Covid-19 pandemic on occupational status, work from home, and occupational mobility. *Journal of Vocational Behavior*, *119*(May), 1–4. https://doi.org/10.1016/j.jvb.2020.103442

Lee, M., & Lan, Y. (2011). Toward a unified knowledge management model for SMEs. *Expert Systems with Applications*, *38*(1), 729–735. https://doi.org/10.1016/j.eswa.2010.07.025

Lovari, A. (2020). Spreading (dis)trust: Covid-19 misinformation and government intervention in Italy. *Media and Communication*, *8*(2), 458–461. https://doi.org/10.17645/mac.v8i2.3219

Manhart, M., & Thalmann, S. (2015). Protecting organizational knowledge: A structured literature review. *Journal of Knowledge Management*, *19*(2), 190–211. https://doi.org/10.1108/JKM-05-2014-0198

Mollenkopf, D. A., Ozanne, L. K., & Stolze, H. J. (2020). A transformative supply chain response to COVID-19. *Journal of Service Management.*, *32*, 190–202. https://doi.org/10.1108/JOSM-05-2020-0143

Obitade, P. O. (2019). Big data analytics: A link between knowledge management capabilities and superior cyber protection. *Journal of Big Data*, *6*(1). https://doi.org/10.1186/s40537-019-0229-9

Pennycook, G., McPhetres, J., Zhang, Y. and Rand, D.G. (2020), Fighting COVID-19 misinformation on social media: Experimental evidence for a scalable accuracy nudge intervention, PsyArXiv [working paper], pp. 1–24.

Probst, G., Romhardt, K., & Raub, S. (2000). *Managing knowledge: Building blocks for success* (pp. 35–232). Wiley.

Renaud, K., Von Solms, B., & Von Solms, R. (2019). How does intellectual capital align with cyber security? *Journal of Intellectual Capital*, *20*(5), 621–641. https://doi.org/10.1108/JIC-04-2019-0079

Renkel, S., Alba, D. and Zhong, R. (2020), Surge of virus misinformation stumps Facebook and Twitter. The New York Times, available at: https://www.nytimes.com/2020/03/08/technology/coronavirus-misinformation-social-media.html, date of access: 10.05.2020.

Ross, C. M. V., & Schulte, W. D. (2005). Knowledge management in a military enterprise: A pilot case study of the space and warfare systems command. In *Creating the discipline of knowledge management* (pp. 157–170). Elsevier.

Singapore Government (2020), https://www.tracetogether.gov.sg/, date of access: 20.05.2020.

Vaccaro, A., Parente, R., & Veloso, F. M. (2010). Knowledge management tools, inter-organizational relationships, innovation and firm performance. *Technological Forecasting and Social Change*, *77*(7), 1076–1089. https://doi.org/10.1016/j.techfore.2010.02.006

van Bavel, J. J., Baicker, K., Boggio, P. S., Capraro, V., Cichocka, A., Cikara, M., Crockett, M. J., et al. (2020). Using social and behavioural science to support COVID-19 pandemic response. *Nature Human Behaviour, Springer US*, *4*, 460–471.

Waizenegger, L., McKenna, B., Cai, W., & Bendz, T. (2020). An affordance perspective of team collaboration and enforced working from home during COVID-19. *European Journal of Information Systems*, *29*(4), 429–442. https://doi.org/10.1080/0960085X.2020.1800417

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, *26*(2), 13–23.

Wei, Y. S., & Wang, Q. (2011). Making sense of a market information system for superior performance: The roles of organizational responsiveness and innovation strategy. *Industrial Marketing Management*, *40*(2), 267–277. https://doi.org/10.1016/j.indmarman.2010.06.039

World Economic Forum, This is the effect COVID-19 will have on global poverty, according to the World Bank, 2020, https://www.weforum.org/agenda/2020/05/impact-of-covid19-coronavirus-economic-global-poverty/, date of access: 10.05.2020.

Zieba, M., & Durst, S. (2018). Knowledge risks in the sharing economy. In E.-M. Vătămănescu & F. M. Pînzaru (Eds.), *Knowledge Management in the Sharing Economy: Cross-sectoral insights into the future of competitive advantage* (pp. 253–270). Springer International Publishing. https://doi.org/10.1007/978-3-319-66,890-1_13

How to cite this article: Zieba, M., & Bongiovanni, I. (2022). Knowledge management and knowledge security—Building an integrated framework in the light of COVID-19. *Knowledge and Process Management*, *29*(2), 121–131. https://doi.org/10.1002/kpm.1707