IFKAD 2021: Managing Knowledge in Uncertain Times
Rome, Italy 1-3 September 2021
ISBN 978-88-96687-14-7 || ISSN 2280-787X

Knowledge Risks in the COVID-19 Pandemic

Susanne Durst*

Tallinn University of Technology,
School of Business and Governance,
Department of Business Administration,
Ehitajate tee 5, 19086, Tallinn, Estonia

Malgorzata Zieba

Department of Management
Faculty of Management & Economics
Gdansk University of Technology
ul.Narutowicza 11/12, 80-233 Gdansk, Poland

Martyna Gonsiorowska

Student of the Faculty of Management & Economics
Gdansk University of Technology
ul.Narutowicza 11/12, 80-233 Gdansk, Poland

** Corresponding author*

Abstract

This conceptual paper aims to identify, present, and analyse potential knowledge risks organizations face in external and dynamic crises such as the COVID-19 pandemic. Until only recently, many researchers and practitioners have perceived knowledge primarily as something positive. This view has changed recently with a growing number of studies highlighting risks related to knowledge. The on-going COVID-19 pandemic can be seen as an additional triggering point which has brought several new knowledge risks. Research on knowledge risks, their consequences and potential ways of handling them is still only in its beginning and consequently rather fragmented. To address this situation, this paper is aimed to provide some theoretical insights into knowledge risks and their possible implications organizations are exposed to in an external and dynamic crisis such as the COVID-19 crisis. To reach this aim, this paper presents a continuation of the research by Durst and Zieba from 2018 related to knowledge risks and their potential outcomes. This present study reviewed the up-dated literature on knowledge risks and uses the taxonomy proposed in the paper by Durst and Zieba to identify and analyse knowledge risks organizations are exposed to in the COVID-19 pandemics. Hence, the paper does not only offer fresh food for thought for researchers dealing with the topic of knowledge risks in the COVID-19 crisis and ways of handling them, it also expands the knowledge risks

ISBN 978-88-96687-14-7 || ISSN 2280-787X

taxonomy proposed by Durst and Zieba; thereby showing both the taxonomy's dynamic character and usefulness.

Keywords – knowledge risks, risk management, knowledge management, knowledge risk management

Paper Type: Academic Research Paper

1 Introduction

This conceptual paper aims to identify, present, and analyse potential knowledge risks organizations face when exposed to external and dynamic crises such as the COVID-19 pandemic. Until only recently, many researchers have perceived knowledge as something positive that has to be shared and disseminated to improve organizational performance (Durst and Edvardsson, 2012; Massingham, 2010). However, this has changed recently with a growing number of studies related to knowledge perceived as a risk, e.g. Durst et al., 2018; Temel and Durst, 2020; Zieba and Durst, 2018. An additional factor that has triggered more knowledge risks is the still on-going COVID-19 pandemic. This crisis represents a new form of an external crisis; one that is dynamic and no end in sight yet (Rapaccini et al., 2020). This new situation has not only forced organizations to rearranging their operations, moving to online work and initiating changes in their normal functioning (Kramer and Kramer, 2020; Mollenkopf et al., 2020; Waizenegger et al., 2020). It has also brought several new knowledge risks. For example, there is a risk of knowledge cherry-picking (some people may select evidence or statistical data so that the information presented agrees with the beliefs of the person making the process). Another example is the risk of deliberate isolation, when a remote employee can naturally lock themselves in their silo, isolate from colleagues, focus on their tasks and not get involved in teamwork, and hence increasing the likelihood of knowledge hiding. There is also the risk that employees are breaking security rules while 'left on their own' (some companies still don't have any special policies for remote workers and there is nothing stopping employees from printing sensitive data from their computers or email files to their private devices). Additionally, many managers and company owners often do not possess skills and tools to accurately assess, examine and manage risks in general (Durst et al., 2021) and knowledge risks in particular. Generally, the research on knowledge risks, their consequences and

ISBN 978-88-96687-14-7 || ISSN 2280-787X

potential ways of handling them is only in its beginning and consequently rather fragmented (Durst and Zieba, 2019). To address fill this situation, this paper is aimed to provide some theoretical insights into the knowledge risks and their possible implications organizations are exposed to in an external and dynamic crisis such as the COVID-19 crisis.

To reach this aim, this paper presents a continuation of the research by Durst and Zieba that has started in 2017 related to knowledge risks and their potential outcomes. It uses the taxonomy proposed by Durst and Zieba to identify and analyse knowledge risks organizations are exposed to in the COVID-19 pandemic. Hence**,** the paper does not only offer fresh food for thought for researchers dealing with the topic of knowledge risks in the COVID-19 crisis and ways of handling them, it also expands the knowledge risks taxonomy proposed by Durst and Zieba; thereby showing both the taxonomy's dynamic character and usefulness.

The paper continues as follows. First, knowledge risks are briefly presented. This is followed by a presentation and discussion of knowledge risks triggered or amplified by the pandemic. The paper terminates with a conclusion section.

2 Knowledge risks – theoretical background

To get deeper into knowledge risk, it is worth getting acquainted with the already developed knowledge risk taxonomy or concept maps. The benefits of concept maps were highlighted by Trochim (1989), it includes expressing the given framework in the language of participants instead of the language of science, which makes the participants more encouraged and helps them to remain on task. A graphic or pictorial product that expresses all major elements and their interrelations is comprehensible to all, it can be presented to the audiences relatively easily and interpreted relatively quickly (Trochim, 1989). Thus, there are also several advantages of creating and analyzing knowledge risks concept maps, reasoned as follows by Durst and Zieba (2019): they are very helpful in visualizing risk, thereby increasing awareness of the knowledge risks and emphasizing their importance, also, concept maps help to understand at what levels in the organization risk is present and how it is related to each other, therefore the holistic view of knowledge in the organization is presented. The map proposed by Durst and Zieba (2019) illustrates the various knowledge risks

ISBN 978-88-96687-14-7 || ISSN 2280-787X

that organizations may face and their interlinkages. On the mentioned map, risk has been classified into three categories: human, technological, and operational.

The human risk category includes the following: "knowledge hiding, knowledge hoarding, unlearning, forgetting, missing/inadequate competencies of organizational members" (Durst and Zieba, 2019, p. 2). Another risk that may fall into this category is the loss of knowledge. Organizations experience a loss of knowledge when a key part of the team leaves the company and takes their experience and expertise with them (Brătianu *et al.*, 2020). All mentioned risks are associated with the individual's behaviors, decisions, intentions, ego, inabilities to learn, forgetting, or missing competencies. The risks associated with technology mapped by (Durst and Zieba, 2019) include "cybercrime, old technologies, digitalization, social media". Ten years ago, only some of the companies relied on the Internet and technology for their business operations, today everyone and every business rely on technology (*The Cost of Cybercrime. Ninth Annual Cost of Cybercrime Study*, 2019), that is why hacker attacks, data theft, old incompatible programs, overreliance on technology, and all dangers related to social media like spreading fake news or trolling accounts are increasing. In the last category, the largest one, the following risks were recognized: "knowledge waste, risks related to knowledge gaps, relational risks, knowledge outsourcing risks, risk of using obsolete/unreliable knowledge, risk of improper knowledge application, espionage, continuity risks, communication risks, knowledge acquisition risks, knowledge transfer risk, and merger & acquisition risks." (Durst and Zieba, 2019, p. 5). This is a very wide category and all the operational risk are still very actual, because even if organizations once implemented knowledge management processes and systems over the past, they may still face operational risks, as it is not enough to coordinate operational knowledge but to identify and manage potential operational risks (Neef, 2005).

3 Knowledge risks in the COVID-19 pandemic

The COVID-19 pandemic has brought enormous challenges to all kinds of organizations. They suddenly faced the need to adapt rapidly to a new work environment and many of them also to remote work. This changed reality has also brought several new knowledge risks. When working remotely, employees are very task-oriented, such a tendency is effective from the point of view of productivity, however, loneliness and the lack of a common work environment

ISBN 978-88-96687-14-7 || ISSN 2280-787X

lead to a decrease in employee engagement and motivation (Mukhopadhyay, 2020). While working remotely many organizations starts to experience some form of 'silos' or already existing silos become even worse. The term "silos" refers to grain silos that separate different types of grain from one another, and therefore is a metaphor for separating different parts of an organization. Moreover, when working from home employees can naturally lock themselves in their silo. According to De Waal, Weaver, Day, & van der Heijden (2019) "the concept of a silo refers not so much to the existence of boundaries, but to the mentality through which those boundaries shape behaviors and ways of working that hinder cross-boundary cooperation and collaboration" (p. xxx). Such 'silo-mentality' even more increases the likelihood of knowledge hiding.

The Covid 19 outbreak, the increased number of persons working from home, and thus the increased internet use have also heightened the risk of cybercrime (Wiggen, 2020). E-mail, social media, video conferences, cloud storage, etc. - all of these have been the order of the day in many companies, but the transition to 100% remote work made that all these tools are used even more and more intensively. Technology remains the key when offices are closed, but it is important to ensure that every employees can access and use the technology properly as much as it is needed for a given workload level (Mukhopadhyay, 2020). Not all employees have been adequately trained on Internet security issues, the risk that employees, due to lack of knowledge, breaks security rules when left on their own increases even more. Home networks, private IT devices, software, and antivirus programs are generally less secure. Overall, it can be concluded that the increasing use of the Internet while working remotely and the growing number of new inexperienced users who have been transferred to the home office suddenly create even more opportunities for criminal activity than before (Wiggen, 2020).

The hurry triggered by the pandemic to switch to home office and remote work has also led to the situation that outdated and underdeveloped IT infrastructures and IT systems clashed with very sophisticated cyber-attacks; thus, technological knowledge risks. This situation has made it even easier for certain individuals/organization to hack themselves in the organizations IT systems to leak sensitive information and knowledge. Given the sophistication of these attacks, many organizations may still have not noticed them. Thus, this situation suggests the presence of both risks related to old technologies and risks of hacker attack (Durst and Zieba, 2018). At the same time, COVID-19 has shown

ISBN 978-88-96687-14-7 || ISSN 2280-787X

that risk management skills are underdeveloped in the majority of organizations (Durst et al., 2021). As a consequence, the initiated responses might have been quick but not decisive.

When considering knowledge risk taxonomy, it can be very useful in the analysis of the present COVID-19 situation in companies.

Beginning with the analysis of the first category – human knowledge risks in the context of the COVID-19 situation, we can notice that some of the threats are more serious than before. For example, knowledge hiding during e-work is even easier, there are less personal contact, face-to-face meeting, and the relation between colleagues are getting worse. There occurs also the risk of deliberate isolation and selfish behaviors of employees. Remote work favors isolation, and remote employees may naturally lock themselves in their comfort zone, focus on their tasks and stop being involved in teamwork and knowledge sharing. Companies are trying hard to bring newer and newer innovations in communication technologies that could have the potential to increase knowledge sharing among co-workers, however, the practices of hiding the knowledge remain prevalent in organizations (Connelly *et al.*, 2019). The same applies to unlearning and forgetting, which have become greater threats in times of remote work. They are more common due to a lack of real contact with co-workers. When a worker does not know something or does not remember, he needs to find out the way to contact somebody who can share the knowledge with him. The whole process of finding out the right person, writing an e-mail, calling someone, or even planning the meeting in advance takes very limited time. Missing/inadequate competencies of organizational members to deal with the new situation is also present in the context of COVID-19. Ignorance of safety rules by employees when working at home can have very negative consequences, such as knowledge losses and leaks.

The next category in the taxonomy is technological knowledge risks, risks that have become even more severe during a pandemic. Beginning with the risk of cybercrime which heightened due to people working at home and using a less secure internet connection or generally speaking less experienced users who break security rules. Moreover, some companies did not have enough time to implement special policies for the remote workers, who may not be aware of special rules and may undertake dangerous actions like printing sensitive data from their computers or sending files to their private devices. Less secured devices and less experienced users can easily be caught by phishing attacks, and

ISBN 978-88-96687-14-7 || ISSN 2280-787X

are a good target for criminal and malicious actors (Wiggen, 2020). The other risks that companies may face are related to old technologies. Some employees may use computers with outdated programs, which means that the program is no longer eligible for producer security updates. For example operating system Windows 7, which Microsoft ended to support at the beginning of the year 2020 is still in use by millions of users (Wiggen, 2020).

Operational knowledge risks are a broad category when considering the knowledge taxonomy. We can also find some examples of this risk in the context of COVID-19. Knowledge transfer is more difficult when limiting to online tools only. Potential gaps when transferring the knowledge can also pose another risk which is improperly applying knowledge. This risk is also affected by missing face-to-face mentoring, difficulties with a concentration of employees, and facing distractions when working at home. The other risk which occurred recently when working remotely is the "silo mentality". Employees when working from home sometimes lose their organizational culture and are not eager to share skills, knowledge, or information with other peoples, teams, or departments, or even to act as "one company"(de Waal *et al.*, 2019). Lack of proper knowledge sharing and information flow may also increase knowledge waste.

Present COVID-19 situation in companies heightened some of the knowledge-related risks in each category of taxonomy.

4 Conclusions

From a theoretical point of view, this study provided evidence of the power and usefulness of knowledge risk map taxonomy proposed by Durst and Zieba. Focusing on knowledge risks triggered by an external crisis, i.e. a pandemic, the taxonomy has shown its dynamic character which can be applied to different scenarios/situations.

From a practical point of view, the study provides useful insight for managers and owners of companies who have understood that any organization is fragile with regard to their knowledge and risks related to it. The recommendations may be useful for business professionals to better handle risks related to knowledge, i.e. to eliminate or alleviate the influence of knowledge risks in the COVID-19 era.

At this stage of development, the proposed study is of theoretical character. This limitation will be addressed in future research activities involving a large

ISBN 978-88-96687-14-7 || ISSN 2280-787X

sample of organizations from various countries and sectors to validate the risks identified or amend them if necessary.

Acknowledgements

The authors greatly acknowledge the financial support from the National Science Centre, Poland, within the grant no. No. 2019/33/B/HS4/02250, entitled "Knowledge risks in modern organizations".

References

Brătianu, C., Nestian, A.S., Tită, S.M., Vodă, A.I. and Gută, A.L. (2020), "The impact of knowledge risk on sustainability of firms", Amfiteatru Economic, Vol. 22 No. 55, pp. 639–652.

Connelly, C.E., Černe, M., Dysvik, A. and Škerlavaj, M. (2019), "Understanding knowledge hiding in organizations", Journal of Organizational Behavior, Vol. 40 No. 7, pp. 779–782.

de Waal, A., Weaver, M., Day, T. and van der Heijden, B. (2019), "Silo-busting: Overcoming the greatest threat to organizational performance", Sustainability (Switzerland), Vol. 11 No. 23, pp. 1–21.

Durst, S. and Zieba, M. (2019), "Mapping knowledge risks: towards a better understanding of knowledge management", Knowledge Management Research & Practice, Vol. 17 No. 1, pp. 1–13.

Durst, S., & Edvardsson, I. R. (2012). Knowledge management in SMEs: a literature review. Journal of Knowledge Management, Vol. 16, No. 6, pp. 879–903. https://doi.org/10.1108/13673271211276173

Durst, S., Bruns, G., & Henschel, T. (2018). The management of knowledge risks: what do we really know? In Global Business Expansion: Concepts, Methodologies, Tools, and Applications (pp. 258–269). IGI Global.

Durst, S., Palacios Acuache, M.M.G. and Bruns, G. (2021), "Peruvian small and medium-sized enterprises and COVID-19: Time for a new start!", Journal of Entrepreneurship in Emerging Economies, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/JEEE-06-2020-0201

Kramer, A., & Kramer, K. Z. (2020). The potential impact of the Covid-19 pandemic on occupational status, work from home, and occupational mobility.

Massingham, P. (2010). Knowledge risk management: a framework. Journal of Knowledge Management, Vol. 14, No. 3, pp. 464–485. https://doi.org/10.1108/13673271011050166

Mollenkopf, D.A., Ozanne, L.K. and Stolze, H.J. (2021), "A transformative supply chain response to COVID-19", Journal of Service Management, Vol. 32 No. 2, pp. 190-202. https://doi.org/10.1108/JOSM-05-2020-0143

Mukhopadhyay, B. (2020), "Managing Remote Work During COVID-19", The Sentinel, No. March, p. 4.

Neef, D. (2005), "Managing corporate risk through better knowledge management", The Learning Organization, Emerald Group Publishing Limited, Vol. 12 No. 2, pp. 112–124.

Rapaccini, M., N. Saccani, C. Kowalkowski, M. Paiola, & F. Adrodegari. (2020). Navigating disruptive crises through service-led growth: The impact of COVID-19 on Italian manufacturing firms. Industrial Marketing Management, 88(July 2020), 225–237. https://doi.org/10.1016/j.indmarman.2020.05.017

Temel, S., & Durst, S. (2020). Knowledge risk prevention strategies for handling new technological innovations in small businesses. VINE Journal of Information and Knowledge Management Systems. https://doi.org/10.1108/VJIKMS-10-2019-0155

The Cost of Cybercrime. Ninth Annual Cost of Cybercrime Study. (2019), .

Trochim, W.M.K. (1989), "An introduction to concept mapping for planning and evaluation", Evaluation and Program Planning, Vol. 12 No. 1, pp. 1–16.

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.

Wiggen, J. (2020), "The impact of COVID-19 on cyber crime and state-sponsored cyber activities", No. 391, p. 11.

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/10.1007/978-3-319-66890-1_13