Knowledge Risks in Organizations – Insights from Companies

Malgorzata Zieba[1], Susanne Durst[2], Martyna Gonsiorowska[1] and Zeynaddin Zralov[1]
[1]Gdansk University of Technology, Poland
[2]Tallinn University of Technology, Estonia
mz@zie.pg.gda.pl
susanne.durst@taltech.ee
martynagon@gmail.com
zzralov@gmail.com
DOI: 10.34190/EKM.21.132

Abstract: Purpose: Knowledge risks are increasingly becoming a great challenge to a variety of organizations. At the same time, academic research on such types of risks, their consequences, and potential ways of overcoming them is still scarce and fragmented. To fill this gap, the paper aims to find out do companies manage their knowledge risks, what are the possible knowledge risks they face and have they observed an increase of knowledge risks during the COVID-19 pandemic. The paper is aimed to present insights on different types of knowledge risks that organizations face, and the ways organizations handle them. The paper also proposes some potential countermeasures organizations might use to mitigate the consequences of knowledge risks. Methodology: The study presents the results of a quantitative survey performed among 60 professionals dealing with management and knowledge risks in organizations. In the study, the authors also have examined what tools and methods are used to manage these risks. The study also explores the level of readiness organizations have to address potential knowledge risks. Findings: The theoretical study has allowed us to identify a variety of knowledge risks, which can bear severe consequences for organizations, such as knowledge loss, knowledge leaking, knowledge hiding, or risks related to cybercrime. All these risks may potentially reduce the productivity in organizations, thus leading to the degradation of organizational performance. Research limitations: Research results are limited to the convenience sample that was selected for the study and thus may not give a comprehensive overview of the state of the art. Practical implications: The study provides useful insights for managers and owners of organizations in need of dealing with the knowledge risks in their organizations. The paper is enriched with a number of sample solutions that they may apply for the sake of their organization. Originality/value: The paper lays the ground for a better understanding of the knowledge risks that organizations need to face nowadays. As such, the paper offers food for thought for researchers dealing with the topic of knowledge risks, knowledge management, and organizational risk management in general.

Keywords: knowledge risks, knowledge management, risk management, quantitative research

1. Introduction

The field of knowledge management has been evolving presently into an enriched understanding of knowledge and its importance for companies. It has been already stated that knowledge is a valuable resource and it is necessary to share it and disseminate it broadly because it brings a positive outcome, like innovations or improved performance (Sáenz et al., 2012; Wang & Wang, 2012); however, this understanding seems to be not full. There is a growing body of research showing that knowledge can also be a risk and might be linked with negative aspects of organizational functioning, such as knowledge loss or knowledge hiding (Susanne Durst & Zieba, 2019b; Zieba & Durst, 2018). Examples of such knowledge risks are cyber risks, where organizations are somehow vulnerable to losing their knowledge or information. Cyber risks have become a greater risk to a variety of organizations (Nicol, 2018; Sallos et al., 2019; Tonn et al., 2019). According to the recent report of Allianz, cyber incidents (e.g. cybercrime, IT failure/outage, data breaches, fines, and penalties) rank as the most important business risk (Allianz Risk Barometer, 2020). Nowadays, with more and more daily business activities running online, especially in the face of the COVID-19 crisis, it is becoming critical for organisations to make sure that no one is trying to steal their knowledge or money (Abomhara & Køien, 2015; World Health Organizaton, 2017). Apart from that, additional risk resides in the potential to damage critical infrastructures, such as power stations, transport networks, or hospitals, but also the exposure of personal data. That is why knowledge risk management and cybersecurity start to play a significant role in many types of businesses and organisations become focused more on data and knowledge security than ever before. They become aware that it impacts their viability as a business while considering what sort of information the business possesses, e.g. customer lists, product lists, accounts, and staff lists, etc. Loss of any of these can have detrimental effects on the business.

Generally, the research on knowledge risks, their consequences, and potential ways of handling them is only in its beginning and consequently rather fragmented (Bratianu, 2018; Susanne Durst et al., 2019; Susanne Durst &

Zieba, 2020). To fill this gap, the paper is aimed to provide some empirical insights into organizations' attitudes towards knowledge risks and their implications.

Taking into account the present state of the art, the paper aims to answer the following research questions: *Do companies manage their knowledge risks? What are the possible knowledge risks they face?* and *have they observed an increase of knowledge risks during the COVID-19 pandemic?*

These questions will be answered by the analysis of the study among 60 employees of Polish and Swedish companies.

The paper develops in the following way. First, an introduction to knowledge risks, and their forms and consequences, if not handled properly, is provided. This is followed by a discussion of the study results on knowledge risks. Finally, the present paper concludes with a discussion and conclusion section.

2. Knowledge risks: theoretical background

The concept of knowledge risk (KR) has been developed through the integration of two areas, i.e. risk management, and knowledge management. The very concept of knowledge risk is not used that often, and the literature on the subject is still not very extensive. The Stanford Encyclopedia of Philosophy (2007) explains that risk refers to situations in which it is possible but there is no certainty that an undesirable event will occur. According to Durst and Zieba (2019b) knowledge risk is "a measure of the probability and severity of adverse effects of any activities engaging or related somehow to knowledge that can affect the functioning of an organization on any level". In other words, knowledge risk is any knowledge-related event that interferes with the functioning of an organization or its competitive position (Thalmann & Ilvonen, 2020). All organizations are exposed to knowledge risks, but not always of the same type or intensity (c.f., Kim & Vonortas, 2014). Even more important, there is an interdependence of risks, i.e., one risk can lead to various other risks (Venkatesh, Rathi, & Patwa, 2015).

As knowledge is recognized as the main source of competitive advantage (Stewart, 1997), organizations need to look at their knowledge management approach to consider the potential risks they may face (Susanne Durst & Zieba, 2019b). Even if the risk cannot be eliminated, we can at least predict it and then implement processes that can reduce its negative impact (Massingham, 2010).

Organizations, regardless of size and type, are exposed to a number of risks related to knowledge which have been categorized by Durst and Aisenberg Ferenhof (2016) as follows:

- risks related to human resources. This category refers to the possible consequences of both voluntary and involuntary turnover and (long-term) absence of organization members because of illness or injury;
- relational risk. This category addresses the probability and consequences of having dissatisfactory cooperation and/or being revealed to opportunistic behavior by partner companies or other parties. This risk can also be triggered by knowledge sharing ending with a strengthened counterparty;
- risks related to decision-making in general. Decision-making is based on outdated knowledge, wrong knowledge, or misapplied knowledge;
- risks related to knowledge gaps. This category covers all moments where an organization learns that there is a mismatch between what it must know, and what it actually does know;
- risks related to outsourcing of business functions, such as certain parts of the marketing or human resources management which increases in the long-term the danger of having unlearned to do the business function yourself and in turn brings the organization in an even greater dependency situation.

On the basis of an in-depth literature review, the following knowledge risks have been identified (Durst & Zieba, 2019; Durst & Zieba, 2017):

Table 1: Definitions of particular types of knowledge risks.

Knowledge hiding	"an intentional attempt to withhold or conceal knowledge that has been requested by another person" (Connelly et al., 2012, p. 65)
Knowledge hoarding	the act of accumulating knowledge that may or may not be shared at a later date (Connelly et al., 2012) and this knowledge has not been asked for by another individual - for example, an employee may keep personal information

	secret as an act of omission that is not addressed to a particular person (Webster et al., 2008)
Unlearning	a type of deliberate forgetting which involves a conscious process of giving up and abandoning knowledge, values, and/or practices which are deemed to have become outdated in an organization (de Holan, 2011)
Forgetting	forgetting can be both accidental (due to bad memory) or intentional (trying to avoid bad habits) (de Holan, 2011)
Missing/inadequate competencies of organizational members	a situation when organization members do not possess the necessary training, experience, skills, capacities to complete the tasks assigned to them (own definition)
Risks related to cybercrime	risks related to cybercrime are connected with the threat of malicious software, either destroying or locking computer systems in organizations (Perlroth et al., 2017)
Risks of hacker attacks	a subform of risks related to cybercrime; a hacker attack is a situation in which an outsider is trying to break into computer systems of organizations, especially to get secret information (own definition)
Risks related to old technologies	risks related to the use of old information technologies, resulting in problems with their functioning and updating (own definition)
Digitalization risks	risks connected with the overuse of digital forms of data and reliance entirely on this form of knowledge (own definition)
Risks related to social media	risks of bringing a number of unplanned or undesired consequences, such as the spread of fake information or the existence of fake social media accounts that troll companies' operations (own definition)
Knowledge waste	not making use of available and potentially useful knowledge in the organization (Ferenhof, Durst, & Selig, 2016)
Risks related to knowledge gaps	a mismatch between what a firm must know, and what it actually does know, which in turn may hamper the firm in meeting its objectives (Perrott, 2007)
Relational risks	the probability and consequences of having dissatisfactory cooperation and/or opportunistic behavior by partners (Delerue, 2005)
Knowledge outsourcing risks	a risk of losing skills and capacities needed to perform central (knowledge) processes (Agndal and Nordin, 2009)
Risk of using obsolete/unreliable knowledge	risks that occur when the out-of-date knowledge is applied in the organizational context/inter-organizational settings or when a company applies unreliable knowledge, for example, received from a malicious source (Zieba and Durst, 2018)
Risk of improper application of knowledge	risks that occur when a company does not have the right skills and abilities to analyze and apply knowledge properly (Zieba and Durst, 2018)
Espionage	"the practice of spying or using spies to obtain information about the plans and activities, especially of a foreign government or a competing company" Merriam-Webster Dictionary
Continuity risks	risks that relate to an organization's ability to maintain its core capabilities over time and to its ability to continue to perform and compete at consistent levels as people come and go (Lambe, 2013)
Communication risks	risks that appear in the process by which information is exchanged between individuals through a common system of symbols, signs, or behavior, such as misinterpretation, broken communication flow, etc. (own definition, based on https://www.merriam-webster.com/dictionary/communication)
Knowledge acquisition risks	risks that relate to an organization's ability to acquire the new knowledge it needs to follow a new strategic direction (Lambe, 2013).
Knowledge transfer risks	risks related to all the potential interruptions in the process of transferring knowledge, e.g., lacking willingness to share knowledge, knowledge stickiness, etc. (Durst & Zieba, 2017)
Merger & acquisition risks	risks related to the phenomena occurring during mergers and acquisitions, such as employee reduction, lack of available knowledge, etc. (own definition)
Integration risks	a subform of merger & acquisition risks - the merger/acquisition of an organization by another organization can lead to the situation that the merged organization is not able to integrate the different knowledge sources in a proper way so that it is usable for the members of the newly formed organization (Durst & Zieba, 2017)

Source: Own compilation based on the sources provided in the table.

On the basis of the above classification and provided definitions of particular terms, it can be seen that there are many types of knowledge risks that organizations may face.

To structure different types of knowledge risks and to show their connections, Durst and Zieba (2018) developed a knowledge risks map. Possible knowledge risks are assigned to human, technological, and operational knowledge risks. Human knowledge risks address risks related to a person and the person's personal, social, cultural, and psychological factors. Technological knowledge risks can be the outcome of using various technologies, including ICTs. These knowledge risks may also be triggered by the continued use of old or outdated software; cyber-attacks may also lead to these risks. Finally, operational knowledge risks cover all the risks which can emerge from an organization's day-to-day business operations. Examples to be named in this area are the consequences of outsourcing certain business functions such as accounting or entering into collaborative activities. The continued use of obsolete knowledge even wrong knowledge in firms' business operations can also lead to knowledge risks related to this area.

Inspired by these three risks related to knowledge dimensions, Temel and Durst (2020), identified and described possible knowledge risks that small firms may encounter when being in the process of adopting and/or applying new radical technological innovations. The authors also proposed a number of countermeasures small firms could use for coping with the risks.

However, still not much is known about what types of knowledge risks are identified, faced, and managed by organizations. To fill this knowledge gap, it is necessary to examine knowledge risks in organizations to answer the above stated research questions.

3. Research method

To answer the research questions, a research tool was prepared and tested among managers and educators in the field of management studies. After making improvements for better clarity and cohesion, the questionnaire was sent out via Qualtrics software to 6000 Polish and 6000 Swedish companies from various sectors and of various sizes. E-mail addresses of the companies were purchased from a professional company. As it is a recent and ongoing survey, so far 57 responses have been collected. Additionally, some of the questions were not answered by all the respondents, therefore, the particular number of responses can be different between the questions. The presented findings are part of a large survey. Only some examined aspects are presented due to the space limitations.

4. Empirical findings

The following presents some descriptive initial findings of the study.

The companies were asked whether they do risk management in general and if yes, does this risk management also consider knowledge risks. The vast majority of companies (77%) claimed that they do risk management in general, whereas nearly one fourth (23%) claimed that they do not manage risk.

When asked if the risk management utilized in the companies considers knowledge risks as well, the majority of the participants (69%) answered positively, and nearly one-third (31%) negatively.

Figure 1: Declared risk management in organizations

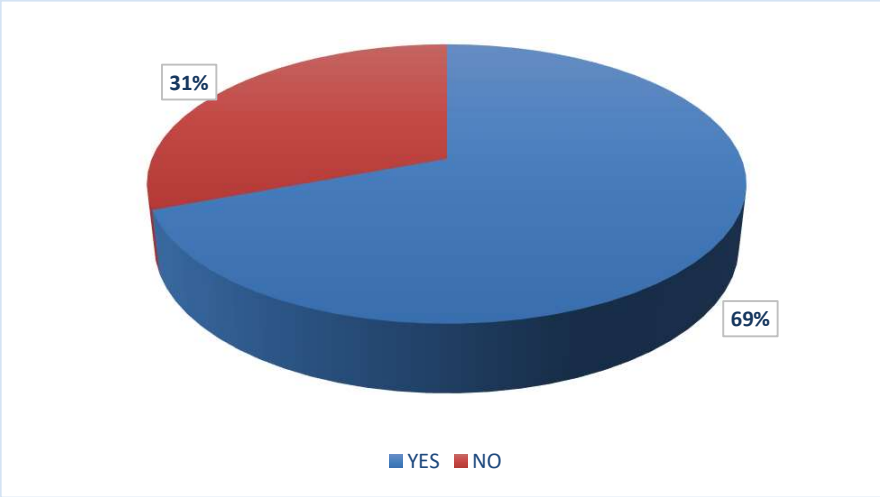

Figure 2: Knowledge risks as part of risk management in organizations

The companies were also asked if they consider the following risks in their risk management:

- Knowledge loss -
- Knowledge leakage
- Knowledge spillover
- Knowledge outsourcing risks
- Risks related to knowledge gaps
- Relational risks
- Risk of using disinformation or unreliable information
- Risk of improper application of knowledge
- Unlearning
- Forgetting
- Knowledge waste
- Knowledge hiding
- Knowledge hoarding
- Risks related to social media
- Risks related to cyber-crime
- Risks related to digitalization

Most of the examined companies (63%) consider knowledge loss and risks related to cyber-crime in their risk management, relational risks are considered in the risk management by 61% of companies, followed by knowledge leakage with 59%, and risk of using disinformation or unreliable information with 56%. The rest of the risks are considered in their risk management by less than half of the companies. That is, risks related to digitalization was recognized by 49% of the participants, risks related to social media by 48%, knowledge outsourcing risks by 46%, risk of improper application of knowledge by 45%, knowledge hiding – by 45%, risks related to knowledge gaps by 37%, knowledge spillover by 37%, forgetting by 37%, knowledge hoarding by 37%, knowledge waste by 35%, and finally unlearning by 27% of the participants.

Figure 3: Consideration of selected knowledge risks in organizations

Additionally, the companies were asked whether the company has been exposed to an increased number of risks since the COVID-19 hit. If yes, they were also asked to specify these risks.

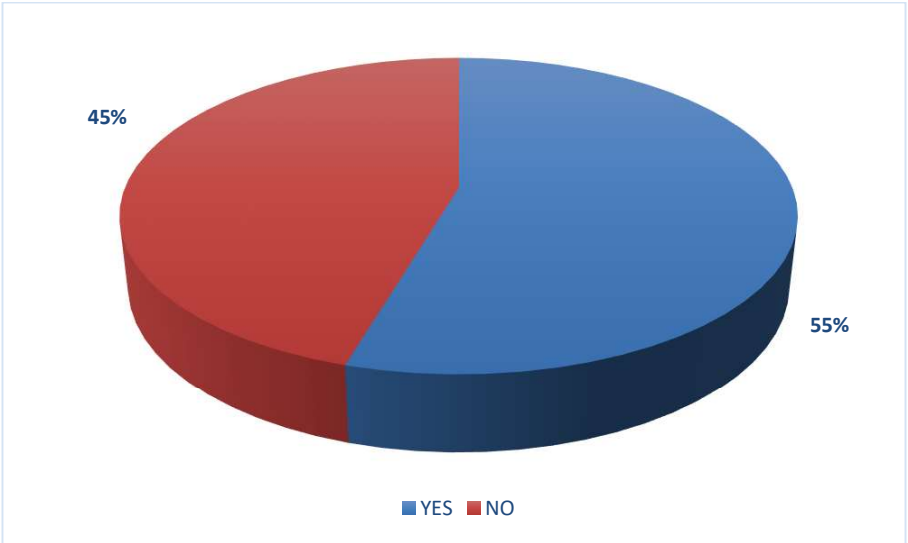

Figure 4: Increased number of risks in the COVID-19 era

More than half of the companies (55%) claimed that their companies have been exposed to an increased number of risks since the COVID-19 hit, while the remaining participants (45%) claimed that the company has not been exposed to an increased number of risks since the COVID-19 hit.

Additionally, the companies were asked to specify the risks related to the COVID-19 pandemic. The collected answers are presented in Table 2.

Table 2: Risks identified by companies in the COVID-19 era

Risks identified by companies:
200 employees in quarantine
Quick infection, drop in income, low employee productivity
Disinformation
Loss of contact with clients
Related to cybercrime - because a large proportion of employees work remotely.
Equipment theft
Treat of leakage of information in connection with remote work of employees
Shutdown by state institutions or due to high absenteeism
Virus infection, staff shortages
Sending sensitive data via email
Bad reputation
Hacker attacks; Hacking the system
Lots of more spam
Risk of cyber-attack, risk of clients not returning to the service once the pandemic and restrictions are over

As it can be seen in the table above, many of the identified risks were related to IT areas, e.g. hacker attacks increased amount of received spam, disinformation, risks of cyber-attacks, etc. There were also a number of human-related risks identified, e.g., high absenteeism, decreased employee productivity, a sudden event of employees in quarantine, etc.

5. Discussion

As those preliminary results show, many companies manage their risks (77%) and a large part of them also considers some knowledge risks as well (69%). The top managed knowledge risks are: knowledge loss, risks related to cyber-crime, relational risks, and knowledge leakage. The least popular risks that companies do not manage or do not know if they manage are: unlearning, knowledge waste, knowledge hoarding, forgetting, and knowledge spillover. More than half of the companies have been exposed to an increased number of knowledge risks since the COVID-19 breakout. Among the ones mentioned by companies were, for example disinformation, hacker attacks, absence of employees due to the quarantine of employees, or even equipment theft. Thus, based on the findings some changes/refinements of Table 1 are possible to acknowledge the somewhat changed risk exposure experienced by the firms during a health crisis (see Table 3). As we have learned the pandemic has led to an increased relevance of risks that can be assigned to the human and technological dimensions in particular (Durst and Zieba, 2019), the content of Table 3 goes into it more intensively.

Table 3: Risk exposure during a health crisis

Human dimension	
Missing/inadequate competencies of organizational members	The pandemic has shown that the majority of organization members did not possess necessary basic training and skills with regard to risk management (crisis management).
High levels of absenteeism	High levels of absenteeism have pushed companies to their limits, the smaller the company the worse. Business operations had to be adjusted downwards accordingly.
Knowledge/information leakage	Remote working has increased the danger of knowledge / information leakage caused intentionally or unintentionally by the organization members.

Risks related to knowledge gaps	A mismatch between what a firm must know, and what it actually does know. A number of these knowledge gaps became apparent during the pandemic -> see "Missing/inadequate competencies of organizational members"
Relational risks	During the pandemic this risk has shown itself as a difficulty in staying in touch with key stakeholders.
Communication risks	Communication is a challenging process; thus, the above-described situation has opened the door for even more misinterpretation, broken communication flow, etc.
Risk of using obsolete/unreliable knowledge	This risk has increased given the spread of fake news/information. Considering the level of sophistication as to which this news/information is spread it has become very difficult to tell the difference between a true and a false report.
Risk of improper application of knowledge	As a consequence of the aforementioned, this risk has increased too.
Knowledge transfer risks	The blurred boundaries between the digital and analog world has further increased this risk.
Knowledge acquisition risks	Given the need for a number of quick changes triggered by the pandemic, this risk has increased too; the acquisition of new knowledge takes time.
Technological dimension	
Risks related to cybercrime	The pandemic has shown that companies are increasingly exposed to this type of risk; especially favored by the crisis-induced rapid digitalization.
Risks of hacker attacks	This sub-form has increased too (see above)
Risks related to old technologies	The rapid digitalization in organizations has amplified this risk even more which in turn has facilitated cyberattacks.
Digitalization risks	Risks connected with the overuse of digital forms of data and reliance entirely on this form of knowledge. The consequences remain to be seen.
Risks related to social media	The increasing use of social media for sharing business related information too has increased the danger of knowledge/information leakage.
Espionage	The race for a COVID-19 vaccine has increased this risk in general. Thus firms being part of vaccine-related supply chains are likely to have been exposed to this risk too.
Organization dimension	
Continuity risks	The consequences of high levels of absenteeism have triggered this risk as the organizations ability to continue to perform its business operations has been challenged. This risk was further amplified by the shutdown of many sectors which put entire business operations to a standstill.

In conclusion, the presented study has provided some interesting insights which should be further strengthened through collecting more data . This would also support in validating the content of Table 3.

6. Conclusions

This study naturally has several limitations. First of all, the research results are limited to the limited sample and therefore, they may not give a comprehensive overview of the state of the art. Second, the term knowledge risk itself is a new term and, as such, may be difficult to be evaluated and examined. Thirdly, some more studies, especially among a greater number of organizations, are necessary to fully understand the present situation, especially in the COVID-19 pandemics. Finally, only one person from the company took part in the survey and therefore, their opinions were not confirmed with other representatives of their organization.

However, the study provides useful insights for managers and owners of organizations in need of dealing with knowledge threats to their organizations. The study also allows managers and owners of companies to understand that any organization can face various types of knowledge risk. The paper lays the ground for future research areas, e.g. examination of knowledge risks in different types of organizations, from various sectors and of various sizes.

All in all, the paper has established the basis for a better understanding of knowledge risks that organizations face nowadays and have to address; the more severe ones in particular. As such, the paper offers food for thought for researchers dealing with the topic of knowledge risks and organizational risk management in general.

Acknowledgements

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

References

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, *4*(1), 65–88. https://doi.org/10.13052/jcsm2245-1439.414

Agndal, H., & Nordin, F. (2009). Consequences of outsourcing for organizational capabilities: Some experiences from best practice. *Benchmarking: An International Journal*, *16*(3), 316–334. https://doi.org/10.1108/14635770910961353

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

Connelly, C. E., Zweig, D., Webster, J., & Trougakos, J. P. (2012). Knowledge hiding in organizations. *Journal of Organizational Behavior*, *33*, 64–88. https://doi.org/10.1002/job.737

de Holan, P. M. (2011). Agency in voluntary organizational forgetting. *Journal of Management Inquiry*, *20*(3), 317–322. https://doi.org/10.1177/1056492611408265

Delerue, H. (2005). Relational risk perception and alliance management in French biotechnology SMEs. *European Business Review*, *17*(6), 532–546. https://doi.org/10.1108/09555340510630563

Durst, S., & Aisenberg Ferenhof, H. (2016) "Knowledge Risk Management in Turbulent Times." In K. North, & Gregorio Varvakis (eds.), Competitive Strategies for Small and Medium Enterprises Increasing Crisis Resilience, Agility and Innovation in Turbulent Times, Springer International Publishing, Cham (pp. 195-209).

Durst, S., & Zieba, M. (2017). Knowledge risks - Towards a taxonomy. *International Journal of Business Environment*, *9*(1). https://doi.org/10.1504/IJBE.2017.084705

Durst, S., Hinteregger, C., & Zieba, M. (2019). The linkage between knowledge risk management and organizational performance. *Journal of Business Research*, *105*(November 2018), 1–10. https://doi.org/10.1016/j.jbusres.2019.08.002

Durst, S., & Zieba, M. (2017). Knowledge Risks – Towards a Taxonomy. *International Journal of Business Environment*, *9*(1), 51–63.

Durst, S., & Zieba, M. (2019a). 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

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

Durst, S., & Zieba, M. (2020). Knowledge risks inherent in business sustainability. *Journal of Cleaner Production*, *251*, 119670. https://doi.org/10.1016/J.JCLEPRO.2019.119670

Ferenhof, H. A., Durst, S., & Selig, P. M. (2016). Knowledge Waste and Knowledge Loss ? What is it all about? *Navus Revista de Gestão e Tecnologia*, *5*(4), 38–57. https://doi.org/10.22279/navus.2016.v6n4.p38-57.404

Kim, Y., & Vonortas, N. S. (2014). Managing risk in the formative years: Evidence from young enterprises in Europe. Technovation, 34, 454–465. doi.org/10.1016/j.technovation.2014.05.004.

Lambe, P. (2013). *Four Types of Knowledge Risk*. http://www.greenchameleon.com/uploads/Four_Types_of_Knowledge_Risk.pdf

Massingham, P. (2010). Knowledge risk management: a framework. *Journal of Knowledge Management*, *14*(3), 464–485. https://doi.org/10.1108/13673271011050166

Nicol, D. M. (2018). Cyber risk of coordinated attacks in critical infrastructures. *Proceedings of the 2018 Winter Simulation Conference*, 2759–2768.

Perrott, B. E. (2007). A strategic risk approach to knowledge management. *Business Horizons*, *50*(6), 523–533. https://doi.org/10.1016/j.bushor.2007.08.002

Sáenz, J., Aramburu, N., & Blanco, C. E. (2012). Knowledge sharing and innovation in Spanish and Colombian high-tech firms. *Journal of Knowledge Management*, *16*(6), 919–933. https://doi.org/10.1108/13673271211276191

Sallos, M. P., Garcia-Perez, A., Bedford, D., & Orlando, B. (2019). Strategy and organisational cybersecurity: a knowledge-problem perspective. *Strategy and Organisational Cybersecurity*, *20*(4), 581–597. https://doi.org/10.1108/JIC-03-2019-0041

The Stanford Encyclopedia of Philosophy (2007)

Stewart, T. (1997). *Intellectual capital: The new wealth of organizations.* Doubleday Currency.

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, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/VJIKMS-10-2019-0155

Thalmann, S., & Ilvonen, I. (2020). Why Should We Investigate Knowledge Risks Incidents? - Lessons from Four Cases. Proceedings of the 53rd Hawaii International Conference on System Sciences, 4940–4949. https://doi.org/10.24251/hicss.2020.607

Tonn, G., Kesan, J. P., Zhang, L., & Czajkowski, J. (2019). Cyber risk and insurance for transportation infrastructure. Transport Policy, 79(March), 103–114. https://doi.org/10.1016/j.tranpol.2019.04.019

Wang, Z., & Wang, N. (2012). Knowledge sharing, innovation and firm performance. Expert Systems with Applications, 39(10), 8899–8908. https://doi.org/10.1016/j.eswa.2012.02.017

Webster, J., Brown, G., Zweig, D., Connelly, C. E., Brodt, S., & Sitkin, S. (2008). Beyond knowledge sharing: Withholding knowledge at work. Research in Personnel and Human Resources Management, 27(08), 1–37. https://doi.org/10.1016/S0742-7301(08)27001-5

World Health Organizaton. (2017). WHO Information Note on the Use of Dual HIV / Syphilis Rapid Diagnostic Tests (RDT). 1–8.

Venkatesh, V. G., Rathi, S., & Patwa, S. (2015). Analysis on supply chain risks in Indian apparel retail chains and proposal of risk prioritization model using interpretive structural modeling. Journal of Retailing and Consumer Services, 26, 153–167. doi.org/10.1016/j.jretconser.2015.06.001.

Zieba, M., & Durst, S. (2018). Knowledge Risks in the Sharing Economy. In Knowledge Management in the Sharing Economy. Cross-Sectoral Insights into the Future of Competitive Advantage (pp. 253–270).