A new Critical risk on the Block: Cyber Risks as an Example of Technical Knowledge Risks in Organizations

Malgorzata Zieba[1], Susanne Durst[2] and Martyna Gonsiorowska[3]
[1]Division of Management - Gdansk University of Technology, Poland
[2]School of Business and Governance, Department of Business Administration, Tallinn University of Technology, Estonia
[3]Student of the Faculty of Management & Economics, Gdansk University of Technology, Poland
mz@zie.pg.gda.pl
susanne.durst@taltech.ee
martynagon@gmail.com

Abstract: The breakout of the COVID-19 pandemic has intensified the appearance of many additional technical knowledge risks in organizations. Cyber risks in particular are becoming a great challenge for organizations. At the same time, academic research on cyber risks, their costs, consequences and ability of overcoming them is still scarce and fragmented. In order to fill this gap, the paper is aimed to identify different types of cyber risks that organizations face and to examine the organizations' ability to handle those risks. The paper presents research results from a sample of 60 organizations, addressing questions such as: (i) What are the costs of cyber risks the organization has faced? (ii) What is the company ability to address these risks?, and (iii) What is the organization doing to minimize the impact of such risks? Data was collected by means of a questionnaire. This research study has allowed to identify the state of the art concerning cyber risks, which can bear severe consequences for organizations. The findings clearly show that not all organizations suffer from the same level of cyber risks but it is much related to their field of operations. Consequently, also the ability to manage these cyber risks is quite diversified among the examined companies. Research results are limited to a sample of 60 organizations and thus the findings should be taken with caution. The study provides useful insights for managers and owners of organizations in need of dealing with the cyber threats/attacks and other technical knowledge risks threatening their organizations. The paper is enriched with a number of sample solutions that they may apply to mitigate those risks.The paper lays the ground for a better understanding of technical knowledge risks, primarily cyber risks, to which organizations are increasingly exposed today. As such, the paper offers food for thought for researchers dealing with the topic of technical knowledge risks and organizational risk management in general.

Keywords: cyber risks, technical knowledge risks, preventive actions, knowledge management

1. Introduction

Knowledge management has been traditionally perceived as a means for organizations to achieve better performance (Inkinen, 2016; Schiuma, 2012), become more innovative (Ferraresi, 2012; Inkinen et al., 2015) or satisfy their customers better (Gibbert et al., 2002), just to name a few examples. In relation to this, knowledge has been considered a valuable resource that needs to be managed, shared, disseminated, etc. (McCann & Buckner, 2004). So far, little attention has been paid to potential risks related to knowledge, although there are some publications available examining some selected knowledge risks, such as knowledge hiding and hoarding (Butt, 2020a, 2020b; Silva de Garcia et al., 2020), knowledge waste and loss (Ferenhof et al., 2015; Ferenhof et al., 2016); or knowledge spillovers (Fernandes & Ferreira, 2011; Rodriguez, 2014).

Although the obvious efforts, in general, the area of knowledge risks, their appearance in organizations, as well as handling them by organizations is still underexplored and there are few publications that present results from studies among organizations (Durst & Zieba, 2020; Zieba, 2020). There are also different kinds of knowledge risks that can be identified in organizations, namely human knowledge risks (e.g. knowledge hiding, unlearning, forgetting), operational knowledge risks (e.g. knowledge waste, risks related to knowledge gaps, knowledge outsourcing risks) and finally, technological knowledge risks (e.g. risks related to cybercrime, risks related to social media).

Taking the above into account, there is a need for more research concerning knowledge risks, also their technological type (e.g. risks related to cybercrime). That is why, the following research questions have been formulated: How well do organizations manage their cyber risks? What is the cost of cyber incidents faced by them? What is their ability to identify, mitigate and overcome these risks? These questions will be answered by the analysis of the study among 60 employees of Polish and Swedish companies.

The paper is organized in the following way. First, an introduction to technical knowledge risks, their forms and threats related to them is provided. Next, the research method is presented, followed by a discussion of the results of the study on cyber risks. Finally, the present paper concludes with a discussion and conclusion section.

2. Technical knowledge risks

Knowledge risk constitutes a new term that is increasingly discussed in the literature. The concept of knowledge risk indicates that although knowledge has always been recognized as something valuable and positive, there are also potentially negative aspects related to knowledge and risks arising from inadequate knowledge management in organizations (Borch, 2022). Knowledge risks has been defined as "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" (Durst & Zieba, 2019, p. 2). Compared to other risks, risks associated with knowledge are (more) difficult to address and, thus, manage. This means a particular challenge for organizations that have no or underdeveloped management systems (Temel & Durst, 2021).

Durst and Zieba (2019) proposed to divide knowledge risks into human knowledge risks, technological knowledge risks, and operational knowledge risks to visualise different types of knowledge risks and their links. This categorization may also help to start a better discussion on the topic of knowledge risks. According to these authors, technological knowledge risks, which is the focus of the present paper, may be the result of the increasing use of various (digital) technologies. While technological risk has received increasing attention over the past few years, the literature is still very scarce. The Global Risks Report 2019, defines technological risks as adverse consequences resulting from technological developments. The report lists and describes risks such as cyber-attacks, data theft, and the collapse of critical information infrastructure (Varonis Data Lab, 2019). These risks are also relevant to knowledge management. Durst and Zieba, in their knowledge classification, assigned risks related to digitalization, old technology, cybercrime, and social media to the technological knowledge risk category (2019). Risks related to cybercrime refer to being exposed to threats of malicious software that destroys or locks the IT system of organizations (Perlroth et al., 2017). Hacker attacks may be considered a sub-form of this risk describing incidents where outsiders are trying to break into the IT systems to get access to confidential information. Possible consequences can be business disruptions or even a halt of the organization's operations. Cyber risks (incidents) rank, according to a report of Allianz, as the most important business risk (Allianz Risk Barometer, 2020), and it has been observed that cybercriminals have taken advantage of the pandemic to deploy ransomware against critical infrastructure and healthcare institutions (Interpol, 2020). Recently, Cybersecurity Ventures reported that the cost of cybercrime globally is expected to be 6 trillion US dollars, and it is expected to increase as high as 10.5 trillion US dollars in 2025.

The potential for all technological risks is further increased due to digitization, the radical changes associated with infrastructure development provide a venue for cyber-attacks but also amplify their potential damage (World Economic Forum, 2019). Any over-reliance on technology and ignoring the human factor can be detrimental to an organization as well (Durst & Zieba, 2019), especially since people are still the weakest link when it comes to cybersecurity and are the cause of successful cyberattacks (Accenture Security, 2019).

3. Research method

To answer the research questions provided in the introduction section, a research tool was prepared and tested among managers and educators in the field of management studies. As the examined topic has not been previously researched, it was not possible to rely on the existing tools and questionnaires. Thus, new items were developed or existing ones from related areas (such as risk management) were adjusted for the purpose of the study. Apart from the parts related to knowledge risks and their management, supplementary demographic data were collected, such as the year of foundation, type of organization, location, or number of employees hired in the company.

After the construction of the questionnaire, it was pretested to check the order of questions, their comprehensibility, and appropriateness to be answered in a certain period (max. 30 minutes). The questionnaire was carefully pretested with two management professors and two respondents from companies to check if the questions are understandable and express the planned outcome.

After making improvements for better clarity and cohesion, the questionnaire was sent through Qualtrics software to 6000 Polish and 6000 Swedish companies of various sectors and of various sizes. The e-mail

addresses of the companies to be conducted were provided by a professional company that offers such services. In the first stage of the survey, 57 responses were collected and they are presented in this paper. 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 constitute a part of a larger survey, and, therefore, only some examined aspects are presented in this paper to examine the research questions and fulfil the aim of the study.

4. Empirical findings

The following presents some descriptive initial findings of the study.

Companies were asked to specify the mean cost of all cyber incidents (in EUR) their company suffered over 12 months. 38% of companies could not specify the cost, 22% claimed that they had 0 costs related to the cyber incidents, 16% of companies reported a cost in the range 1-10000EUR, 9% in a range 10001-20000EUR, and 7% estimated their cost between 20001-30000EUR. 5% of companies reported that their cost exceeds 40000EUR, and 3% estimated their cost between 300001-40000EUR.

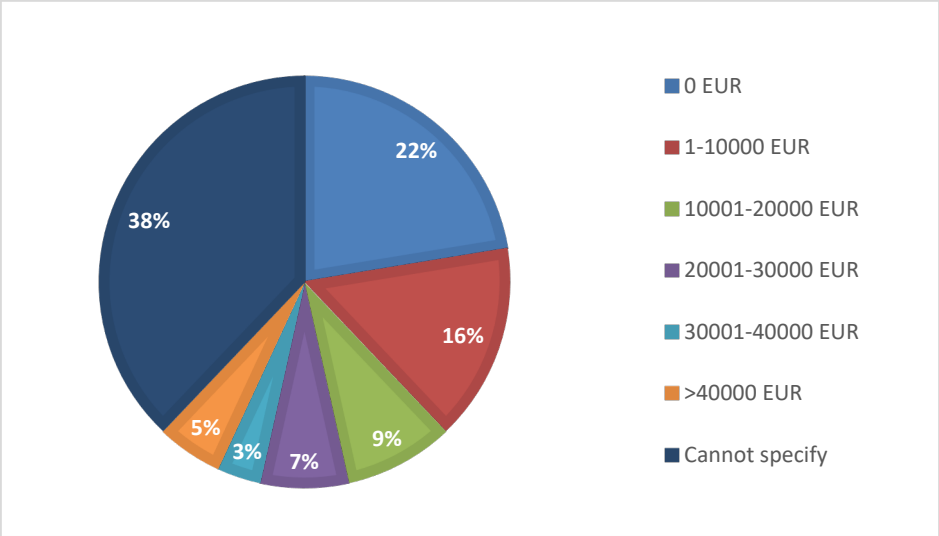

Figure 1: Declared mean cost of all cyber incidents (in EUR) their company suffered for 12 months.

Furthermore, companies were asked to specify the mean cost of the largest single cyber incident (in EUR) their company suffered over 12 months. 41% of companies could not specify the cost, 22% claimed that they had 0 costs related to the cyber incidents, 21% reported a cost in the range 1-10000EUR, 7% in the range 10001-20000EUR. 5% of companies reported that their cost exceeds 40000EUR, 2% estimated their cost between 20001-30000EUR, and 2% between 300001-40000EUR.

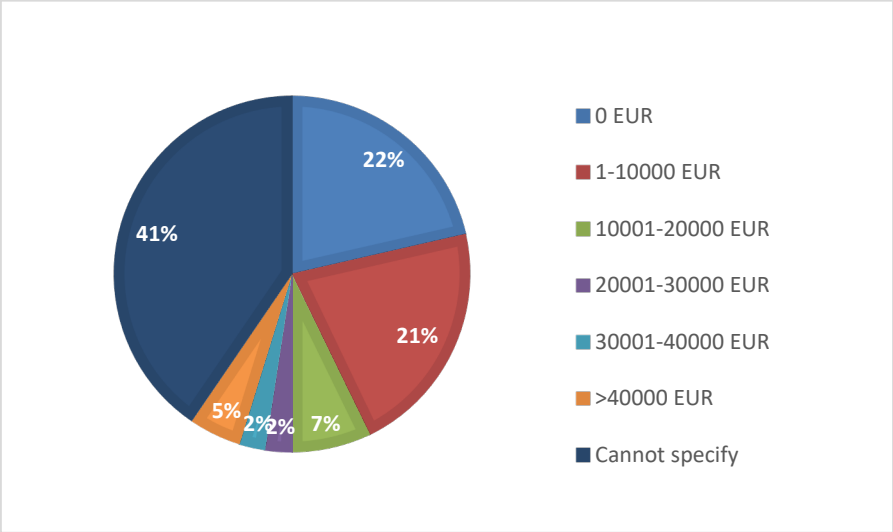

Figure 2: Declared mean cost of the largest single cyber incident (in EUR) their company suffered over 12 months

In addition, companies were asked to assess their ability to address cyber risks. Most (56%) rated themselves intermediate, 24% as experts, 11% as novices, and 9% did not know how to assess themselves.

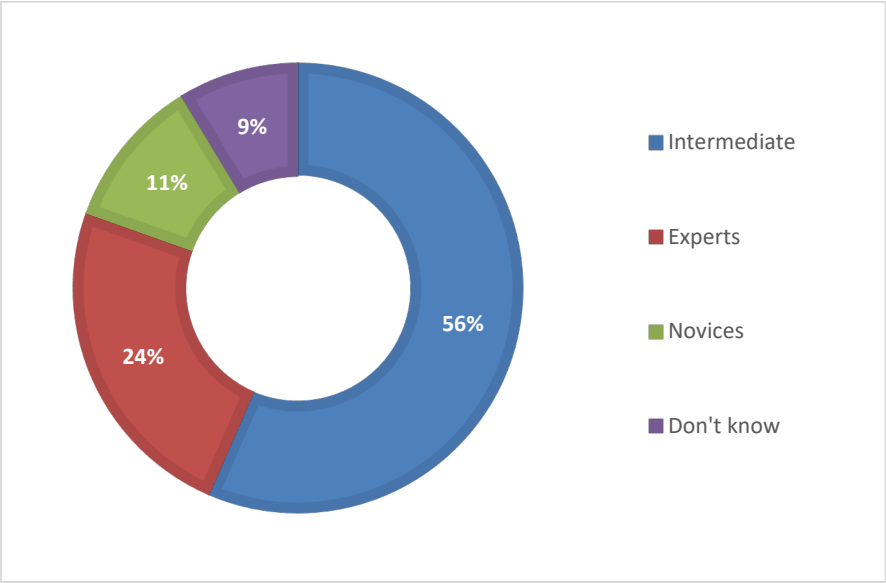

Figure 3: Declared ability to address cyber risks

Companies were also asked to assess the priority of cyber risks among the organization's risk management priorities. More than half of companies (55%) consider cyber risk in the top five, 21% recognize the risk of cybercrimes, but do not rank it in the top five of their risk management priorities. 13% of the companies claimed that cyber risk in their hierarchy has low priority, 7 % did not know how to assess the risk, and only 4 % of the respondents recognized cyber risk as the number one risk.

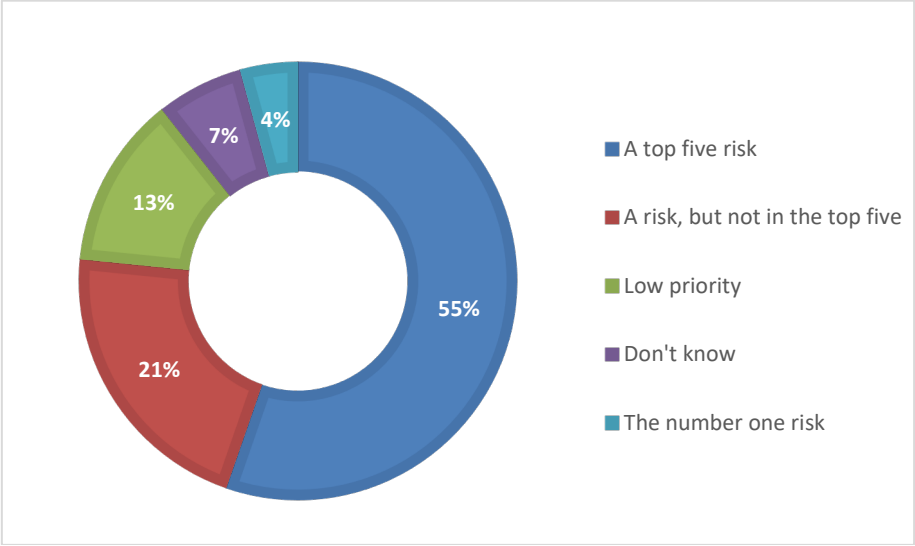

Figure 4: Declared position of cyber risk among the organization's risk management priorities

When asked about the confidence of an organization regarding identifying and assessing cyber risks, 35 % of companies answered that they feel fairly confident, 30% highly confident, 20% not at all confident, and 15% did not know.

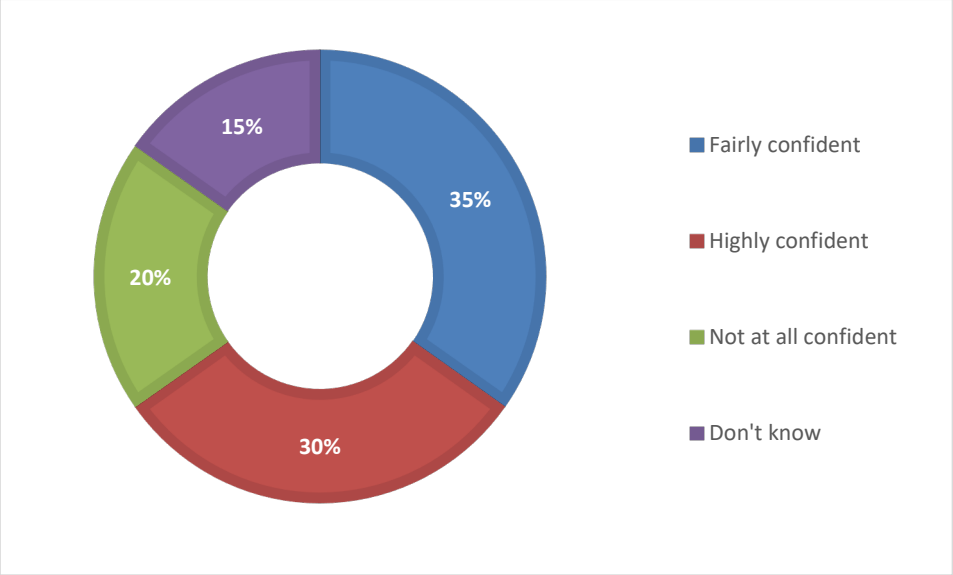

Figure 5: Declared confidence regarding identifying and assessing cyber risks

Respondents were also asked to assess the confidence of the organization in mitigating and preventing risks. 40 % of companies feel fairly confident with this activity, 30% are highly confident, 17% are not at all confident, and 13% did not know how to answer the question.

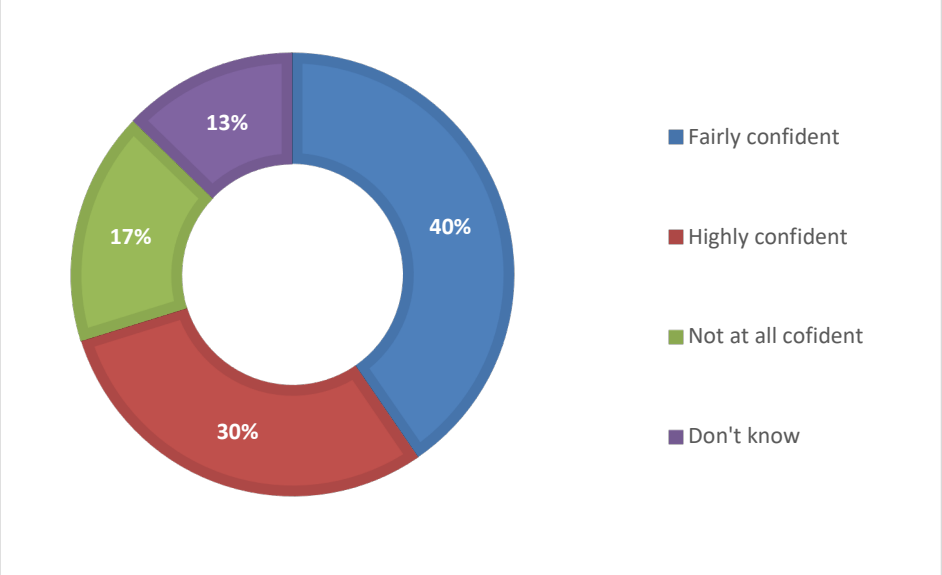

Figure 6: Declared confidence regarding mitigating and preventing cyber risk

When asked about, the confidence of an organization regarding respond to cyber risks and recovering from them, almost half of the companies (47%) claimed that they are fairly confident, 25% claimed highly confident, 15% did not know how to answer, and 13% claimed that they are not at all confident.

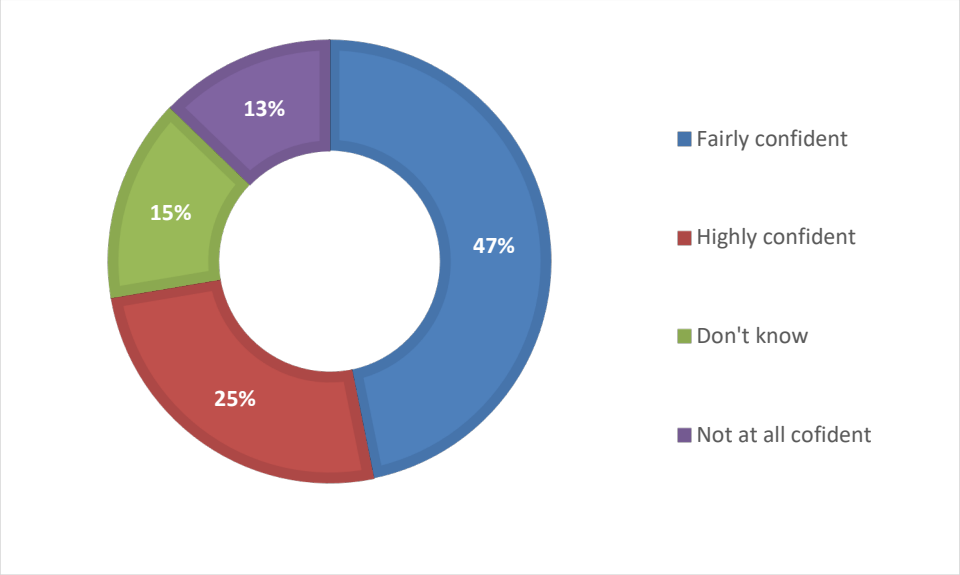

Figure 7: Declared confidence regarding responding to cyber risk and recovering from it

5. Discussion

What is quite interesting and surprising is that more than one third of the examined companies were not able to provide the declared mean cost of all cyber incidents (in EUR) their company suffered for the last 12 months, as well as the declared mean cost of the largest single cyber incident (in EUR) their company suffered over 12 months. This situation can result from several factors. First, it is possible that their companies do not measure the costs of such cyber incidents or that this kind of information is kept secret by the management. Second, ever the cost of such cyber incidents might be difficult to be estimated and calculated, for example how to measure the cost of an employee having their social media account hacked. Third, employees themselves might be reluctant to inform their superiors about potential incidents due to the fear of receiving reprimand or even being fired. All those factors are worth further examination and the implementation of some mechanisms in organizations to overcome potential threats, for example by supporting the knowledge sharing culture and blame-free reporting.

As far as the declared ability to address cyber risks is concerned, most companies declared themselves intermediate, while only one fourth as experts. This might indicate that there is still a lot to be done in organizations to become better experts in fighting cyber risks and there is a need for more knowledge absorption on how it can be done.

At the same time, examined companies seemed to understand the importance and significance of cyber risks and the majority of them indicated these types of risks as one of the top five risks. Additional more than one fifth declared it is an important risk, but out of top five. This can show an increasing awareness of the threats related to cyber risks that is noticeable in companies – perhaps they have already noticed those risks and their potential severity, yet they have not introduced any special measures to examine their impact. This may be consistent with the picture presented above of the increasing threats from cybercrime noticed by organizations examining it.

Examined companies also indicate high confidence in identifying, assessing, mitigating, preventing, responding, and recovering from cyber risks. Around two thirds of the examined companies declared that they are fairly or highly confident with regards to these risks. This might be a bit too optimistic picture, especially when analyzed together with the indicated lack of knowledge on the cost of cyber-attacks. Perhaps companies are over confident now, as they have not experienced severe attacks yet and they will modify their approach either by being less confident or keeping the confidence level, but also upskilling in the area of cyber risks and their handling.

Taking into account the fact that organizations have been facing cyber risks, as well as other technical risks, it is important to provide them with some ways to handle those risks. Examples of such ways as: application of

protection mechanisms (e.g. installation and actualization of anti-virus software; keeping the software updated; password management application, etc.); crucial data duplication in various locations; support from professional agencies in case of high risk faced by an organization; up-date of technologies, when required and advised (Durst and Zieba, 2020).

6. Conclusions

This paper provides some information on cyber risks and their management in organizations. More precisely, it describes insight into cyber risk management in Polish and Swedish organizations of different sectors and sizes. Based on a diverse sample that included 60 organizations from both countries, the findings show that cyber risks have become a key risk that organizations must deal with. Regarding the perception of the organization's competences and skills to manage this type of risk, the findings suggest differences between the surveyed organizations that could possibly be attributed to the nature of the company's activity.

This study naturally has several limitations that can be drawn into future research avenues. First of all, the study of preliminary character and more responses are needed to present a broader picture. Second, the cultural differences have not been taken into consideration here due to the place limitation; however, they may constitute a natural area of future examination. Third, the study presented here is just a part of the larger research undertaking and therefore, does not present the full picture of the knowledge risks in organization. It is though important to note that the limitations of the paper are a good starting point for future explorations and studies. Future studies could examine the execution of both qualitative and quantitative studies (even mixed methods approaches) to identify and examine relevant cyber risks and their influence on business sustainability in particular types of companies (e.g. knowledge-intensive organizations vs. production companies). Researchers could also design and investigate longitudinal research projects to study the potential contribution of applied KRM to various operations and outcomes of organizations (e.g. innovativeness, agility, etc.).

Acknowledgements

The study was supported by a 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

Accenture Security (2019). The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study. *Ninth Annual Cost of Cybercrime Study*, 18. Retrieved from https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

Allianz Risk Barometer,(2020). Identifying the major business risks for 2020. url: https://www. agcs. allianz. com/content/dam/onemarketing/agcs/agcs/reports. *Allianz-Risk-Barometer-2020. pdf*.

Borch, C. (2022). Machine learning, knowledge risk, and principal-agent problems in automated trading. *Technology in Society*, *68*(January), 101852. https://doi.org/10.1016/j.techsoc.2021.101852Butt, A. S. (2020a). Consequences of top-down knowledge hiding: a multi-level exploratory study. *VINE Journal of Information and Knowledge Management Systems*. https://doi.org/10.1108/VJIKMS-02-2020-0032

Butt, A. S. (2020b). Mitigating knowledge hiding in firms: an exploratory study. *Baltic Journal of Management*, *15*(4), 631–645. https://doi.org/10.1108/BJM-01-2020-0016

Interpol (2020). The International Criminal Police Organization. https://www.interpol.int/How-we-work/COVID-19

Cybercrime Magazine (2020). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025* https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

Durst, S., & Zieba, M. (2019). Mapping knowledge risks: towards a better understanding of knowledge management. *Knowledge Management Research and Practice*, *17*(1), 1–13. https://doi.org/10.1080/14778238.2018.1538

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.., 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

Ferenhof, H., Durst, S., & Selig, P. (2015). Knowledge Waste in Organizations: a Review of Previous Studies. *Brazilian Journal of Operations & Production Management*, *12*(1), 160–178. https://doi.org/10.14488/BJOPM.2015.v12.n1.a15

Fernandes, C., & Ferreira, J. J. (2011). Knowledge Spillovers and Knowledge Intensive Business Services: An Empirical Study. *Economic Policy*, *2116*, 0–26. https://doi.org/10.1227/01.NEU.0000349921.14519.2A

Ferraresi, A. a. (2012). Knowledge management and strategic orientation: leveraging innovativeness and performance. *Journal of Knowledge Management*, *16*, 688–701. https://doi.org/10.1108/13673271211262754

Gibbert, M., Leibold, M., & Probst, G. (2002). Five Styles of Customer Knowledge Management, and How Smart Companies Use Them To Create Value. *European Management Journal*, *20*(5), 459–469. https://doi.org/10.1016/S0263-2373(02)00101-9

Inkinen, H., Kianto, A. & Vanhala, M. (2015). Knowledge Management Practices and Innovation Performance in Finland. *Baltic Journal of Management*, *10*(4), 432–455.

Inkinen, H. T. (2016). Review of empirical research on knowledge management practices and firm performance. *Journal of Knowledge Management*, *20*(2).

McCann, J. E., & Buckner, M. (2004). Strategically integrating knowledge management initiatives. *Journal of Knowledge Management*, *8*, 47–63. https://doi.org/10.1108/13673270410523907

Perlroth, N., Scott, M., & Frenkel, S. (2017). *Cyberattack Hits Ukraine Then Spreads Internationally (Published 2017)*. The New York Times. https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html

Rodriguez, M. (2014). Innovation, knowledge spillovers and high-tech services in European regions. *Engineering Economics*, *25*(1), 31–39. https://doi.org/10.5755/j01.ee.25.1.3207

Schiuma, G. (2012). Managing knowledge for business performance improvement. *Journal of Knowledge Management*, *16*(4), 515–522. https://doi.org/10.1108/13673271211246103

Silva de Garcia, P., Oliveira, M., & Brohman, K. (2020). Knowledge sharing, hiding and hoarding: how are they related? *Knowledge Management Research and Practice*, *00*(00), 1–13. https://doi.org/10.1080/14778238.2020.1774434

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*.

Varonis Data Lab. (2019). *2019 Global Data Risk Report From the Varonis Data Lab*. 28.

World Economic Forum. (2019). Global Risks Report 2019. In *Geneva Switzerland*.

Zieba, M. (2020). Knowledge Risk Management in Companies Offering Knowledge-Intensive Business Services. In S. Durst & T. Henschel (Eds.), *Knowledge Risk Management* (pp. 13–31). Springer.