The Impact of Knowledge Vulnerabilities on Knowledge Risks

Constantin BRATIANU[11]
Ruxandra BEJINARU[22]
Vlad-Mihai URSACHE[33]

Abstract

The purpose of this paper is to explore the impact of knowledge vulnerabilities on knowledge risks and to analyse their intricate connections within the knowledge management systems. It is a new topic in knowledge management which is requested by the accelerated process of digitalization and the exponential development of the AI programs. There is a lack of research in this area and efforts should be made to bridge the knowledge gap. The method we use is based on a critical analysis of knowledge vulnerabilities and knowledge risks within a generic organization and of designing tree-diagrams able to illustrate the connections between them, and the possible adverse consequences for the firm's performance. The method of tree-diagrams has been extensively used in risk analysis of the complex technological systems of airplanes and nuclear reactors. Also, it is used in the risk management applied to other domains like climate change and earthquakes. It is the first paper to investigate these phenomena and to conceptualize such kind of diagrams.

Keywords: *knowledge dynamics, vulnerability, knowledge vulnerability, risk, knowledge risk, knowledge management*

JEL classification: D81, D83, D84

DOI: 10.24818/RMCI.2024.1.70

1. Introduction

Knowledge vulnerability is a new concept that hardly can be found in the knowledge management literature (Bratianu & Bejinaru, 2022). Also, *knowledge risk* is a relatively new concept, although there are some papers trying to explain it in the context of knowledge management (Durst, 2019; Durst & Henshel, 2020; Durst & Zieba, 2020). However, the correlation between knowledge vulnerabilities and knowledge risks have not been analysed so far. This is the first paper using the tree-

[1] Constantin Bratianu, Bucharest University of Economic Studies, Romania, constantin. bratianu@gmail.com

[2] Ruxandra Bejinaru, „Stefan cel Mare" University of Suceava, Romania. ruxandrab @usm.ro

[3] Vlad-Mihai Ursache, National University of Political Studies and Public Administration, Bucharest, Romania. ursachevladmihai@yahoo.com

diagram logic to show the impact of knowledge vulnerabilities on knowledge risks and their possible adverse consequences.

2. Literature Review

Knowledge became in the last decades a strategic resource that contributes significantly to achieve competitive advantage and business sustainability (Bratianu & Lefter, 2001; Massingham, 2020; Nastase, 2007; Nicolescu & Nicolescu, 2022; Nonaka & Takeuchi, 2019). As demonstrated by Bratianu (2022), *knowledge* is an intangible resource that should be understood as a nonlinear field composed of rational knowledge, emotional knowledge and spiritual knowledge. Each form of knowledge can be transformed into another form, generating a continuous dynamics that influences managerial decision making (Bratianu & Bejinaru, 2020). *Knowledge management* is the management of intangible resources and their dynamics within a given organization or any other form of a social entity (Massingham, 2020; North & Kumta, 2018). *Knowledge management systems* represent the functional framework of any organization. They are composed of people, technology and processes. The performance of any knowledge management system impacts on the organizational performance and its business sustainability.

Knowledge vulnerabilities represent the weak parts or functional aspects of a knowledge management system. They are potential factors able to generate *knowledge risks* under some external forces, leading this way to some possible adverse consequences for the firm and its performance (Bratianu & Bejinaru, 2022; Massingham, 2010). The concept of vulnerability is well-known in other research domains like climate change and natural hazards analysis (Fuchs, Birkman & Glade, 2012; McCarthy et al., 2001), but it is quite new in knowledge management systems (Bejinaru, 2022).

Vulnerabilities may be called potential internal threats. They are latent properties of a certain system and became active under some internal or external forces acting upon that system. For instance, any computer that is not protected by an antivirus software has a potential vulnerability towards viruses which may destroy some databases or block the normal operations. That vulnerability can be decreased or even eliminated by providing for that computer a powerful antivirus software. In the climate change domain, the concept of vulnerability is defined as "the degree to which a system is susceptible to, or unable to cope with effects of climate change, including climate variability and extremes" (McCarthy et al., 2001, p. 995). Searching for vulnerabilities is not so easy because it requires a high level of understanding how a system works and how it responds to external forces and unexpected changes in the business environment, like political, social and economic crises.

Knowledge vulnerabilities are the roots of *knowledge risks* and they become active during unfavourable changes form the external business environment. Although vulnerabilities and risks are related through a causal logic, they are not symmetrical phenomena, such that "reduced vulnerability always means reduced outcome risk, but reducing the outcome risk does not always reduce vulnerability" (Sarewitz, Pielke & Keykhah, 2003, p. 809).

Knowledge risk can be defined starting from the generic formula of risk and considering the uncertainty due to the absence of knowledge. Therefrore, we can say that the *risk* of a certain knowledge event R(i) is given by the product between the *probability* of happening that event P(i) and the *consequences* associated with the realization of that risk C(i) (Zieba & Durst, 2018). It is a direct application of the concept of *risk* to a knowledge management system:

$$R(i) = P(i) \text{ x } C(i) \qquad (1)$$

where: P(i) represents the probability of happening the event (i), and C(i) stands for the possible adverse consequence of that event. P(i) can be computed from detailed statistics concerning the event (i), when these statistics are available. When they are available, then we assign subjective probabilities based on our experience and judgment. The same situation happens for evaluating the magnitude of all possible adverse consequences. For natural hazards like earthquakes, floods or hurricanes there are usually statistics to compute the necessary distribution of probabilities, but for knowledge risks such kinds of data is missing from most of the firms. Therefore, for computing knowledge risks it is necessary to use experience and qualified judgment coming from managers and experts in the field of knowledge management and risk management (Bratianu et al., 2020; Bratianu, Stanescu & Mocanu, 2021; Massingham, 2020).

The risks are always related to *uncertainty* due to the absence of knowledge (Spender, 2014). Uncertainty is a characteristic of the future because of the practical impossibility of knowing what will happen then and of the lack of necessary information and knowledge. Uncertainty is mostly subjective due to different perceptions coming from different people on the same possible events. Ignorance is a personal attribute, and interpreting uncertainty is directly related to each individual level of ignorance. Therefore, uncertainty reveals a relationship between each individual and his external environment (Lindley, 2006). Events may have objective probabilities, but their perception is based on previous experience of each individual and on his beliefs (Holton, 2004). Education induced in our minds that we have to learn certain packages of information and knowledge due to some linear and deterministic thinking patterns. However, the knowledge universe is infinite and nonlinear. Therefore, we never can dispose of all the knowledge we need to reach a state of certainty. That leads to the idea of accepting for each of us a lack of knowledge, or a certain level of ignorance leading to uncertainty (Bernstein, 1998).

Due to their business education focused on economic principles and profit maximization, managers developed a bias for rationality and rational knowledge risks (Durst, 2019; Durst & Henshel, 2020; Durst & Zieba, 2020). However, we need a holistic perspective in understanding knowledge risks and their potential harm to firm’s performance. The holistic perspective can be achieved only if we start our research with the paradigm of knowledge fields and knowledge dynamics (Bratianu & Bejinaru, 2019, 2020). Thus, we consider the rational knowledge field, emotional knowledge field, spiritual knowledge field, and their dynamics in the process of decision making under conditions of uncertainty (Hill, 2008; Kahneman, 2011). Therefore, we can identify three large categories of knowledge risks: rational knowledge risks, emotional knowledge risks, and spiritual knowledge risks (Bratianu, 2018). Due to knowledge dynamics we cannot make a clear cut between these categories, but researchers should look for the dominant form of knowledge.

There are many taxonomies concerning knowledge risks (Bratianu et al., 2020; Durst, 2019; Durst & Zieba, 2019; Massingham, 2010). The most recent one (Zieba, Durst & Gonsiorowska, 2022) classifies knowledge risks into three categories: human, operational and technological. The most important risks are: knowledge loss, knowledge hiding, knowledge hoarding, unlearning, forgetting, and knowledge leaks. The operational knowledge risks are related directly to the processes within a given firm. They are: knowledge acquisition risks, adequate application of procedures, lack of experience, lack of understanding some new operations. The technological knowledge risks refer mostly to the information systems and to possible penetration of them by some hackers or viruses. Cybersecurity is a whole new domain developed to identify and manage such kinds of risks in order to reduce their possible damages. El Khatib, Ali and Mostapha (2021) keep the three categories mentioned above and introduce *strategic knowledge risks* as a new category, where they consider those risks which have a long standing impact on firm’s performance like knowledge loss, knowledge leakage and knowledge gap.

Bratianu (2018) creates a new taxonomy taken as a classifying criterion the basic fields of knowledge, as shown in Table 1.

Knowledge risks taxonomy based on knowledge fields

Table 1

Categories of knowledge risks	Types of knowledge risks
Rational knowledge risks	knowledge loss, knowledge leakage, cybersecurity risks, improper use of operational procedures, obsolete technology, forgetting, unlearning, knowledge transfer, improper application of knowledge
Emotional knowledge risks	conflicts with organizational culture, conflicts with managers, knowledge hiding, knowledge hoarding, lack of a rewarding system, lack of mutual respect
Spiritual knowledge risks	conflicts with organizational values, changes in organizational values, focus exclusively on profit maximization, no meaning in work, change in the leadership style

Regardless of the taxonomy used, one of the most important knowledge risk is knowledge loss (Bratianu, 2018; Bratianu & Bejinaru, 2022; Durst and Zieba, 2019, 2020; Zieba, Durst & Gonsiorowska, 2022). Knowledge loss is related to the departure of any employee from the firm due to the retirement age or to a certain degree of dissatisfaction (Nastase et al., 2022). It is a loss of explicit and tacit knowledge, and consequences can be severe when there is a significant percentage of people leaving in the same time. That can be seen from the knowledge balance of the whole firm:

$$\Delta K = \Delta KC + \Delta KA - \Delta KL \qquad (2)$$

In this equation, ΔK stands for the variation of the knowledge level of the firm, ΔKC represents the variation induced by knowledge creation, ΔKA is the variation due to knowledge acquisition, and ΔKL is the variation due to knowledge loss.

The importance of the knowledge loss risk is very well demonstrated by DeLong (2004) analysing many cases from big American firms. The case of Boeing became almost a reference for knowledge loss, as a result of a wrong retirement strategy. Therefore, knowledge loss can create severe production and financial problems. Another example analysed by DeLong (2004) is that of NASA. Due to many re-structuring schemes and downsizing decisions due to cost-cutting strategy, NASA lost a significant amount of its critical knowledge for designing and constructing space vehicles. However, knowledge loss is not only about rational knowledge. When a significant number of people leave a firm, they take with them a set of values and attitudes which may influence the emotional and spiritual distribution of knowledge within the firm, changing this way its knowledge entropy. Moreover, if some of the employees who leave the firm go to another firm, the consequence can be a lost in knowledge uniqueness and its contribution to competitive advantage.

3. Methodology

This is a conceptual paper based on a critical literature review, on mapping knowledge vulnerabilities and risks within a firm and on analysing the causal relationships between them. Our research is transferring the logic of conceptualizing a tree-diagram from risk management toward knowledge risk management (Krajewski, Ritzman & Malhotra, 2007). A tree-diagram represents a linear translation of a complex phenomenon that is nonlinear such that we can understand the cause-effect impact of vulnerabilities and anticipate the possible consequences through knowledge risks. The value of the tree-diagrams resides in their explicit illustration of the most probable connections between knowledge vulnerabilities, knowledge risks and their possible consequences. In an advanced stage of research, the tree-diagrams can be completed with probabilities and evaluation of the magnitude of possible consequences. Then, these tree-diagrams serve in designing knowledge strategies to minimize knowledge vulnerabilities and their impact on knowledge risks. Also, managers can design emergent strategies to decrease the damages generated by the possible knowledge risks.

4. Discussion and results

Designing tree-diagrams for the knowledge vulnerabilities and risks should be based on the following axioms:

a) The diagram is a linearization of a nonlinear process by extracting from it the significant cause-effects relationships.
b) The relationships between knowledge vulnerabilities and knowledge risks are not unique. Therefore, one knowledge risk can be generated by the contribution of several knowledge vulnerabilities, and one knowledge vulnerability can generate several knowledge risks.
c) The relationship between one knowledge vulnerability and one knowledge risk is not symmetric. Therefore, reducing the magnitude of a certain knowledge vulnerability contributes to the decrease of the associate knowledge risk, but the reverse is not true.
d) Tree-diagrams can be generic instruments for analysing any knowledge management system, but when they are completed with probabilities, they become specific for each firm. Knowledge risk probabilities distribution is specific for each firm.

Let us think which knowledge vulnerabilities can contribute to generate the knowledge loss (KL) risk in a generic firm. Figure 1 shows that we can identify three main vulnerabilities: a high percentage of employees retiring in the same time (RK), experts leaving the firm due to their dissatisfaction with the firm's management (EK), and the attitude of hiding knowledge due to a fierce individual competition between employees (HK).

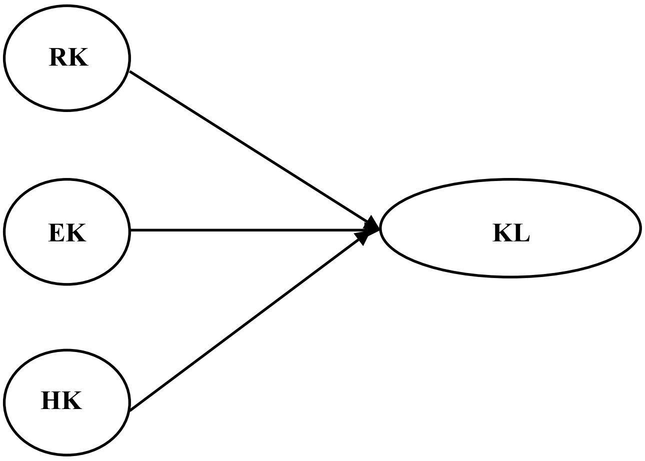

Figure 1. Knowledge vulnerabilities impact on knowledge loss risk

Source: Authors' own research

While we explained the impact of retiring employees and experts leaving the firm on knowledge loss, the knowledge hiding vulnerability is a more complex phenomenon. There is a certain dynamics between knowledge sharing and knowledge hiding in each employee as a result of the psychological climate created within given firm. If there is a clear strategy for encouraging knowledge sharing, with a well-defined rewarding system, and there is no threat for losing power, people will share a good part of their knowledge with their team colleagues, and knowledge hiding is relatively low. However, if there is fierce competition between individuals and no rewarding system for knowledge sharing, the level of knowledge hiding will be high. From this point of view, that knowledge cannot be distributed and cannot be used by other employees. Therefore, that hidden knowledge will have a negative influence on innovation and problem-solving. It is like a knowledge loss because it can be used only by its owner, and only in those situations when he is playing a certain role in making decisions. Furthermore, knowledge hiding increases knowledge loss when the owner of that knowledge leaves the firm. In conclusion, knowledge hiding is an important vulnerability for a firm, contributing to the knowledge loss risk. Figure 2 illustrates how knowledge hiding vulnerability generates a whole tree of knowledge risks and their associated adverse consequences.

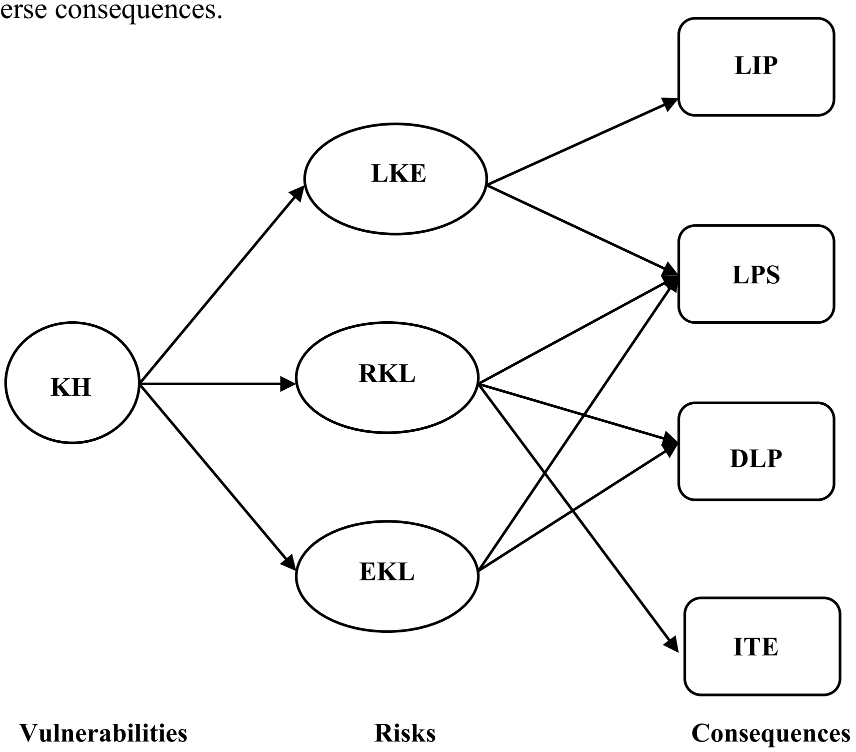

Figure 2. Tree-diagram for the knowledge hiding vulnerability
Source: Authors' own research

In figure 2 we used the following notations: KH – knowledge hiding; LKE – low knowledge entropy; RKL – retired knowledge loss; EKL – experts knowledge loss; LIP – low innovation process; LPS – low problem-solving capacity; DLP – danger of losing projects; ITE – investment in training new employees. The tree-diagram can be complicated much more, but its complexity might be difficult for adequate interpretation. Therefore, the complexity of a tree-diagram is a trade-off between usefulness in designing knowledge strategies and mapping the real phenomena as accurate as possible. Researchers can use focus groups or in-depth interviews to obtain some quantitative evaluations for a certain firm and complete this diagram with numbers. Then, its usefulness is enhanced and managers will have a valuable instrument to think how to decrease knowledge vulnerabilities and risks, such that their impact on the firm's performance to decrease significantly.

5. Conclusions

The purpose of this paper is to analyse the correlations between knowledge vulnerabilities, knowledge risks and their consequences within a generic knowledge management system, and to design a tree-diagram for those correlations. Therefore, the paper bridges a gap in the knowledge management literature and adds value through this new perspective. Knowledge vulnerabilities are those weak elements in a knowledge management system which generate knowledge risks under some internal or external adverse conditions. They are the roots of knowledge risks and any analysis of knowledge management systems should incorporate methods for identification and evaluation of these vulnerabilities and risks.

Research focused so far only on knowledge risks and only of the level of constructing different taxonomies and identifying different type of risks. Risks are generated by any uncertainty state of a generic knowledge management system and therefore the number and types of knowledge risks could be infinite. Researchers should increase their level of analysis beyond creating taxonomies by trying to reveal the intricate connections between knowledge vulnerabilities and knowledge risks, and to conceptualize tree-diagrams for mapping those cause-effect relationships.

The value of this paper resides in applying for the first time the tree-diagram method used in risk management to the knowledge management systems. The complexity of such diagrams can be increased by considering all identified knowledge vulnerabilities within a generic firm, anticipating all possible knowledge risks generated by these vulnerabilities and evaluating the magnitude of possible adverse consequences associated with those knowledge risks.

The limitation of this method comes from the fact that a tree-diagram represents a linear structural model of some nonlinear phenomenon which means assuming a series of approximations. Knowing the degree of these approximations is important and helps in designing solutions for mitigating the adverse consequences of knowledge risks.

References

1. Bejinaru, R. (2022). Cluster analysis of risks and vulnerabilities for environment sustainable management. *Oradea Journal of Business and Economics,* 7(2), 35-48. https://doi.org/10.47535/1991ojbe155**.**
2. Bersntein, P.L. (1998). *Against the Gods: The remarkable story of risk*. John Wiley & Sons, New York.
3. 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**.**
4. Bratianu, C. (2022). *Knowledge strategies*. Cambridge University Press, Cambridge.
5. Bratianu, C. & Bejinaru, R. (2019). The theory of knowledge fields: A thermodynamics approach. *Systems*, 7(2), 1-12. https://doi.org/10.3390/systems7020020**.**
6. Bratianu, C. & Bejinaru, R. (2020). Knowledge dynamics: A thermodynamics approach. *Kybernetes*, 49(1), 6-21. https://doi.org/10.1108/K-02-2019-0122.
7. Bratianu, C. & Bejinaru, R. (2022). Exploring vulnerabilities and risks related to knowledge management systems. In: Schiuma, G. & Bassi, A. (Eds.). *Proceedings of the 17th International Forum for Knowledge Asset Dynamics* (pp. 687-700), SUPSI University, 20-22 June 2022, Lugano, Switzerland.
8. Bratianu, C. & Lefter, V. (2001). *Management strategic universitar*. Editura RAO, Bucuresti.
9. Bratianu, C., Nestian, A.S., Tita, S.M., Voda, A.I. & Guta, A.L. (2020). The impact of knowledge risk on sustainable of firms. *Amfiteatru Economic*, 22(55), 639-652. https://doi.org/10.24818/EA/2020/55/639**.**
10. Bratianu, C., Stanescu, D.F. & Mocanu, R. (2021). Exploring the knowledge management impact on business education. *Sustainability*, 13(4), 2313, 1-16. https://doi.org/10.3390/su13042313**.**
11. DeLong, D.W. (2004). *Lost knowledge: Confronting the treat of an aging workforce.* Oxford University Press, Oxford.
12. Durst, S. (2019). How far have we come with the study of knowledge risk? *VINE Journal of Information and Knowledge Management Systems*, 49(1), 21-34. https://doi.org/10.1108/VJIKMS-10-2018-0087**.**
13. Durst, S. & Henshel, T. (2020). *Knowledge risk management: From theory to praxis.* Springer Nature, Berlin.
14. 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/14778238.2018.1538603.
15. Durst, S. & Zieba, M. (2020). Knowledge risks inherent in business sustainability. *Journal of Cleaner Production*, 251, Art. 119670, 1-10. https://doi.org/10.1016/j.jclepro.2019.119670**.**
16. El Khatib, R.A., Ali, A.E.A. & Mostapha, N. (2021). A review of knowledge risks conception. *BAU Journal – Creative Sustainable Development*, 3(1), Art. 9, 1-9.
17. Fuchs, S., Birkman, J. & Glade, T. (2012). Vulnerability assessment in natural hazards and risk analysis: Current approaches and future challenge. *Natural Hazards,* 64, 1969-1975. https://doi.org/10.1007/s11069-012-0352-9.

18. Hill, D. (2008). *Emotionomics: Leveraging emotions for business success*. Revised Edition. Kogn Page, London.
19. Holton, G.A. (2004). Defining risk. *Financial Analysis Journal*, 60(6), 19-25.
20. Kahneman, D. (2011). *Thinking, fast and slow*. Strauss, Giroux and Farrar, New York.
21. Krajewski, L.J., Ritzman, L.P. & Malhotra, M.K. (2007). *Operations management: Processes and value chains.* 8th Edition. Pearson, Upper Saddle River.
22. Lindley, D.V. (2006). *Understanding uncertainty*. Wiley-Interscience, New York.
23. Massingham, P. (2010). Knowledge risk management framework. *Journal of Knowledge Management,* 14(3), 464-485.
24. Massingham, P. (2020). *Knowledge management: Theory and practice*. SAGE, Los Angeles.
25. McCarthy, J.J., Cauziami, D.F., Leary, N.A., Dokken, D.J. & White, K.S. (Eds.). *Climate change 2001: Impacts, adaptation and vulnerability*. Cambridge University press, Cambridge.
26. Nastase, M. (2007). *Lideri, leadership si organizatia bazata pe cunostinte*. Editura ASE, Bucuresti.
27. Nastase, M., Ciobanu, Gh., Ganea, O., Gombos, C.C. & Popescu, L.N. (2022). Approaches to occupational mobility under the conditions of the current economic crisis. *Review of International Comparative Management*, 23(5), 578-589. https://doi.org/10.24818/RMCI.2022.5.578.
28. Nicolescu, O. & Nicolescu, C. (2022). *Stakeholder management and social responsibility: Concepts, approaches and tools in the covid context*. Routledge, New York.
29. Nonaka, I. & Takeuchi, H. (2019). *The wise company: How companies create continuous innovation*. Oxford University Press, Oxford.
30. North, K. & Kumpta, G. (2018). *Knowledge management: Value creation through organizational learning*. 2nd Edition. Springer, Cham.
31. Sarawitz, D., Pielke, R. & Keykhah, M. (2003). Vulnerability and risk: some thoughts from a political and policy perspective. *Risk analysis*, 23(4), 805-810. https://doi.org/10.1111/1539-6924.00357**.**
32. Spender, J.C. (2014). *Business strategy: Managing uncertainty, opportunity, and enterprise.* Oxford University Press, Oxford.
33. Zieba, M. & Durst, S. (2018). Knowledge risks in the sharing economy. In: Vatamanescu, E.M. & Pinzaru, F. (Eds.). *Knowledge management in the sharing economy* (pp. 253-270). Springer International Publishing, Cham.
34. Zieba, M., Durst, S. & Gonsiorowska, M. (2022). Don't forget the dark side of green transformation. In: In: Schiuma, G. & Bassi, A. (Eds.). *Proceedings of the 17th International Forum for Knowledge Asset Dynamics* (pp. 701-709), SUPSI University, 20-22 June 2022, Lugano, Switzerland.