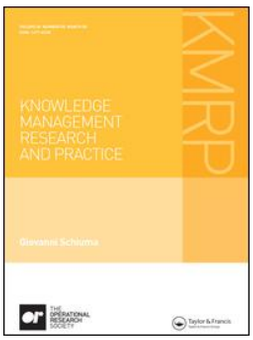

Taylor & Francis
Taylor & Francis Group

Knowledge Management Research & Practice

ISSN: 1477-8238 (Print) 1477-8246 (Online) Journal homepage: http://www.tandfonline.com/loi/tkmr20

Mapping knowledge risks: towards a better understanding of knowledge management

Susanne Durst & Malgorzata Zieba

To cite this article: Susanne Durst & Malgorzata Zieba (2018): Mapping knowledge risks: towards a better understanding of knowledge management, Knowledge Management Research & Practice, DOI: 10.1080/14778238.2018.1538603

To link to this article: https://doi.org/10.1080/14778238.2018.1538603

Published online: 26 Oct 2018.

KNOWLEDGE MANAGEMENT RESEARCH & PRACTICE
https://doi.org/10.1080/14778238.2018.1538603

ORIGINAL ARTICLE

OPEN ACCESS Check for updates

Mapping knowledge risks: towards a better understanding of knowledge management

Susanne Durst[a] and Malgorzata Zieba[b]

[a]School of Business, University of School of Business, University of Skövde, Skövde, Sweden; [b]Management, Gdansk University of Technology, Gdansk, Poland

ABSTRACT

This conceptual paper aims to identify, present, and analyze potential knowledge risks organizations might face. With the growing complexity of organizational environments and the plethora of new knowledge risks emerging, this critical but under-researched field of knowledge management (KM) deserves closer attention. The study is based on a critical analysis of the extant literature devoted to knowledge risks, discusses potential outcomes of these risks and proposes a concept map of knowledge risks. The map shows a number of knowledge risks organizations should be aware of. Knowledge risks can be assigned to three categories: human, technological and operational. The research is the first systematic and comprehensive review of knowledge risks at the organizational level. By aggregating and consolidating the knowledge risks covered, the study does not only provide a knowledge risk taxonomy but also promising directions for future research. The study also contributes to a more comprehensive understanding of KM.

ARTICLE HISTORY
Received 7 December 2017
Revised 19 June 2018
Accepted 17 October 2018

KEYWORDS
Knowledge risks; knowledge management; knowledge risk management; taxonomy; concept map

1. Introduction

Two recent hacker attacks in May and June 2017 have caused severe damage to many countries worldwide, paralyzing not only companies (e.g. Cadbury, Maersk, Merck) but also public institutions (e.g. the old Chernobyl nuclear plant in Ukraine, British hospitals). The attacks in May have spread to more than 74 countries and affected mostly countries like Russia, Ukraine, India, and Taiwan (Perlroth, Scott, & Frenkel, 2017). These attacks reminded us that the digital realm has opened the door to a new number of knowledge risks (KR). In fact, we have learned that new knowledge risks are no longer limited to data and leaks – the digital realm – but increasingly involve the physical realm as well (Perlroth et al., 2017). Additionally, the characteristics of the Internet (speed, reach, anonymity and lack of inherent security) make the emergence of new knowledge risks, e.g. knowledge risks associated with digitalization very easy.

Until recently, knowledge has primarily been perceived as something positive which organizations have to manage to make the best out of it (Durst, 2012; Massingham, 2010; Stam, 2009). The development of knowledge management (KM) field has evolved in the direction of KM practices, processes, activities, and other potential tools and measures to support organizations in achieving this objective (Alavi & Leidner, 2001; Chatzoudes, Chatzoglou, & Vraimaki, 2015; McAdam, 2000). Thus, organizations have mainly concentrated on finding and developing the right knowledge and using it to their advantage.

However, in the face of fast-evolving KR, this focus no longer seems to be sufficient. Organizations need to reconsider their approaches to KM in order to include potential KR they may face as well. Indeed, an effective knowledge (risk) management is needed to make a possible rapid strategic change to address previously held assumptions about what it takes to succeed.

At the same time, the literature on KR is rather scarce and fragmented (Durst & Zieba, 2017; Lee, Suh, & Lee, 2014). There are some studies available, but they present only selected knowledge risks and thus uneven insights, e.g. knowledge loss (Durst & Wilhelm, 2011), (Massingham, 2008), knowledge leakage (Mohamed et al., 2007), knowledge waste (Ferenhof, Durst, & Selig, 2015) or knowledge hiding (Cerne, Nerstad, Dysvik, & Skerlavaj, 2014; Connelly, Zweig, Webster, & Trougakos, 2012). The authors of the present paper argue that both researchers and practitioners should be able to identify and understand a comprehensive number of potential KR and have an overview to capture knowledge in its entirety. Against the background of knowledge and its centrality to organizations, there is an urgent need for a taxonomy of KR. In fact, the

CONTACT Susanne Durst susanne.@his.se School of Business, University of School of Business, University of Skövde, Skövde, Sweden

need for creating a KR taxonomy can be reasoned as follows:

(1) To improve the awareness and significance of KR. A KR taxonomy can help in understanding what a knowledge risk is and how it is interlinked with company operations. It also helps in eliminating the confusion about knowledge risks, which can be characteristic of a new concept.
(2) To have a more holistic view of knowledge in organizations, that is, knowledge being both an asset or a liability (a risk). Thus, an integrative approach towards knowledge and its (risk) management will be possible.
(3) To offer academics the needed ground for encouraging more rigor research on both knowledge risks and knowledge risk management.
(4) To offer practitioners a diagnostic tool to verify whether they have addressed crucial KM aspects (which include KR) to use the potential of knowledge at its best.

The present paper aims to fill a gap in the extant literature by identifying and analyzing a number of essential knowledge risks at the organizational level, together with their links and relations. The organizational level has been chosen because in the aggregate it impacts organizational success. Building on knowledge risks that have been reported in the literature, which can be divided into three categories: namely human, technological and operational knowledge risks, the outcome of our work is synthesized in a knowledge risk map, which is also the main contribution of the paper. This map intends to complement the theory of KM and establish the necessary basis for further research. In addition to being a useful framework for researchers, the map also benefits practitioners and their KM efforts.

The paper is organized as follows. In the next section, the term KR is defined, different knowledge risks and consequences of knowledge risks are described. Then, the development of the KR map is presented, followed by discussion and conclusion section. Finally, section 5 discusses the study's limitations and possible research avenues.

2. Knowledge risks

Knowledge risk is a term that is seldom defined in the literature. One definition found was proposed by Perrott (2007) who describes a knowledge risk as a likelihood of any loss resulting from the identification, storage or protection of knowledge that may decrease the operational or strategic benefit of a company. In the opinion of the authors of the present paper, this definition needs further elaboration. First, the term "risk" should be defined. According to Haimes (2009), risk is "a measure of the probability and severity of adverse effects (i.e., consequences)" (p. 1648). When analyzing risks, one should determine: "What can go wrong?", "What is the likelihood?" and "What are the consequences?" (Kaplan & Garrick, 1981). Transferring this general approach towards risks in the field of KM, the following definition is proposed: *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.*

Depending on its origin, the authors of this paper argue that knowledge risks can be classified into the following categories: human, technological and operational. Human knowledge risks are connected with an individual´s personal, social, cultural and psychological factors and thus human resources management. For example, the risk of knowledge hiding is related to the human dimension of knowledge risks. Technological knowledge risks result from the usage of various technologies, including information and communication technologies (ICT), but are not limited to those. Risks from this category may be the outcome of or initiated by, for example, the use of old technologies or hacker attacks. Finally, the operational category of knowledge risks embraces all the risks resulting from everyday operations and functioning of organizations, e.g. making alliances or mergers, outsourcing, applying wrong or obsolete knowledge in operations. Like any risk, knowledge risks should be managed, acknowledging that they cannot be eliminated.

In the following sections, the identified knowledge risks will be discussed.

2.1. Human knowledge risks

In the following, knowledge hiding, knowledge hoarding, unlearning, forgetting, missing/inadequate competencies of organizational members will be discussed.

3. Knowledge hiding

Knowledge hiding can be defined as "an intentional attempt to withhold or conceal knowledge that has been requested by another person" (Connelly et al., 2012, p. 65). According to (Connelly & Zweig, 2014), many employees do share all their knowledge because of being afraid to lose their competitive advantage, status or power, while others are afraid of being evaluated by others. Employees may be more prone to hide their knowledge when this knowledge is complex, when it is not task-related and when there is no

climate of sharing in the organization (Connelly et al., 2012). Knowledge hiding is a deliberate approach in the sense that an employee, for some reason, does not want to reveal the possessed knowledge and hides it on purpose. Knowledge hiding is negatively related to innovative work behaviour (Černe, Hernaus, Dysvik, & Škerlavaj, 2017).

4. Knowledge hoarding

Knowledge hoarding is a relatively new and unexplored topic in the literature (Holten, Hancock, Persson, Hansen, & Hogh, 2016). Knowledge hoarding can be defined as 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). Knowledge hoarding is a potential problem in many organizations, as it decreases knowledge sharing and influences organizational culture. It was observed that "employees suffered from knowledge hoarding when they themselves required help, that encouraged them to hoard knowledge themselves, and so the vicious circle began, with all employees losing out" (Why knowledge transfer…, 2017). Among the main reasons why employees hoard their knowledge are: financial incentives, personal ego, and discontent or frustration with the company (Leonard, 2014).

5. Unlearning

According to Lee and Sukoco (2011), "unlearning is understood as both a process and an attitude (outcome)…" (p. 412). Even though "little consideration has been given to unlearning" (Becker, 2008, p. 89), some researchers highlight the importance of the process of unlearning as an antecedent to new learning, related to innovation and organizational changes (Lei, Slocum, & Pitts, 1999). While other authors view unlearning as a phenomenon separated from learning (e.g., Tsang & Zahra, 2008), suggesting that these processes require different skills (Zahra, Abdelgawad, & Tsang, 2011). Unlearning can be viewed as 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). While the deliberate processes of unlearning are considered as being positive they may lead to negative consequences as well in that sense that next to the intentional loss of knowledge, knowledge may also be lost accidentally. For example, a company may unlearn to becoming a multi-cultural company, i.e., a company that accepts different cultural viewpoints and ways of working.

6. Forgetting

Forgetting can be both accidental (due to bad memory) or intentional (trying to avoid bad habits) (De Holan, 2011). Thus, forgetting knowledge can occur because it is seldom used; even though it is relevant knowledge, for example, forgetting how to run a specific tax function of the accounting software. This, in turn, stresses the need for having knowledge repository in place to make sure that the explicit knowledge is captured at least. On the other hand, organizations may try to deliberately forget certain kinds of behavior that hamper them from operating in the desired way, e.g. certain routines that slow down the decision-making process unnecessarily. Similar to the discussion presented in the context of unlearning, forgetting bears the risk that relevant knowledge is being forgotten which would require the organization to relearn it once more or to buy in from outside.

7. Missing/inadequate competencies of organizational members

This risk is related to organization members that do not possess the necessary training, experience, skills, capacities to complete the tasks assigned to them. For example, due to missing experience, mistaken connections are made during the analysis of (new) data by an employee. Another example could be that the manager is drawing wrong conclusions about the impact of a new technology on the company's current offerings. Depending on the situation, the action can generate devastating effects on the organization.

A recent study by PWC (2016) has revealed a huge gap between the IT competencies of board members and the relevance assigned to business technologies (BT). The delegation of BT-related decisions to the IT department is no solution at all.

Setting inadequate priorities to address information overload may be another potential risk threatening a company's objectives. Missing/inadequate competencies may also be the result of missing/inadequate succession planning in organizations (Durst & Wilhelm, 2012) which increases the danger of knowledge attrition or even knowledge loss in the worst case. Additionally, ignorance and negligence on the side of the organization members (both managers and employees) create the likelihood of risks related to knowledge, e.g., careless sharing of sensitive company information and knowledge.

7.1. Technological risks

Risks related to cybercrime, old technologies, digitalization, and social media were assigned to this dimension.

8. Risks related to cybercrime

According to Oxford Living Dictionaries, cybercrime refers to "criminal activities carried out by means of computers or the Internet". It can also be used as a tool to commit an offense (e.g., child pornography, hate crimes) Techopedia (https://www.techopedia.com/definition/2387/cybercrime.) Risks related to cybercrime are connected with the threats of malicious software either destroying or locking computer systems in organizations. By opening an email or its appendix, the victim initiates the software which for example encrypts his/her data, locks them out of their systems and demands ransoms (Perlroth et al., 2017). Such software may spread very quickly, and all the organization's computers might be affected within a moment. This is a serious risk, especially for organizations handling and storing fragile and sensitive data and basing their operations on computer-stored knowledge (e.g., hospitals, governments).

A sub-form of risks related to cybercrime is the ***Risk of hacker attacks.*** A hacker attack is a situation in which an outsider is trying to break into computer systems of organizations, especially in order to get secret information. These attacks can alter data and content and undermine their integrity. Possible consequences can be business disruptions or even a halt. Examples are the alternation of hospital records that causes medical staff to give patients the wrong medicine or stock-trading systems that falsely report changes in stock prices.

9. Risk related to old technologies

An additional risk that can be assigned to technological risks is the risk related to the use of old information technologies. The organization may still use Windows XP even though the support for this computer operating system ended on April 8 2014. A likely consequence is that other software programs used by the organization are no longer being updated to make sure that there is a fit between the programs, i.e. that they remain functioning. In the case of failures, this leads to high costs and long recovery times.

What is observable in public and private organizations is that they have difficulty in keeping up with the immense ICT developments. For example, programs are used that work on technologies that were developed in the early phases of the ICT developments when data security was not an issue compared to today. In the same vein, early versions of the internet were used by academics sharing research data and using the internet for commercial gain was frowned upon (The Economist, 2017).

Additionally, companies might not understand the need to protect their resources with the use of new technologies and solutions, for example, new antivirus software. The applied solutions might be out-of-date and not offering full protection.

10. Digitalization risks

According to the consulting company Gartner, digitalization is the use of digital technologies to change a business model and provide new revenue and value-producing opportunities; it is the process of moving to a digital business (Gartner, 2018).

The increasing usage of algorithms (e.g. in stock markets, or by companies such as Amazon) also has the potential for creating harm as these algorithms can be manipulated, repurposed or deleted, which in turn creates the risk of using disinformation or unreliable information. Consequences are easy to imagine. An overemphasis on the power of algorithms in organizations may even lead to the danger that a questioning of the data/patterns provided come to a halt. Any type of overreliance on the technology, ignoring the human factor, can be harmful to organizations.

11. Risk related to social media

Social media are characterized by "easy searching, open participation, a minimal publishing threshold, dialogue, community, networking, and the rapid and broad spread of information and other content via a wide range of feedback and linking systems" (Aula, 2010). Apart from providing many positive impacts on organizations, social media also possess the danger 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 company's operations.

The underlying notion of social media to encourage information sharing and joint knowledge creation (user-generated content) also support the dissemination of fake news and alternative facts. Automated tools and bots enhance the latter even stronger. An example can be a fake commercial of a real Polish hotel announcing the possibility to win a week at the place created on Facebook and immediately widely disseminated by many Facebook users. To win this stay users had to send an SMS that appeared to be expensive; 30,75 Polish zloty, which is approximately 7,15 Euro. When they found out it is a fake, they were dissatisfied, and the reputation of the hotel was hindered (Polsat News).

11.1. Operational risks

Next, the following risks are discussed: 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.

12. Knowledge waste

Knowledge waste can be defined as not making use of available and potentially useful knowledge in the organization (Durst & Aisenberg Ferenhof, 2016). In such an organization, it is rather likely to expect a continued process of reinvention, which can involve a risk that issues that were already done right cannot easily be replicated/reinvented and thus, the organization may lose (or unlearn) certain strengths over time. At the organizational level, valuable resources are wasted (e.g., human work, financial investments, etc.), as the knowledge that is available is not being used. The level of potential knowledge waste depends on the knowledge not being used in organizations and also on the importance of knowledge for organization's operations.

13. Risks related to knowledge gaps

Perrot (2007) refers to knowledge gaps as 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. In the context of recent ICT developments, it is rather likely that many organizations have a lack of knowledge that would be required both for assessing the potential of different ICT tools in general and the possible fields of application as well as implications of these tools. Coming back to the issue of succession, the exit of an individual can also lead to this knowledge gap as a previously available skill may no longer available in the organization. Also, this type of risk may lead to an overestimation of the company's own capabilities (Lambe, 2013).

14. Relational risks

Relational risk is the probability and consequence of having dissatisfactory cooperation and/or opportunistic behavior by partners (Delerue, 2005). In addition, it comprises the risk of knowledge sharing, which may end in the strengthening of the partner at the expense of the company's own competitive standing (Coras & Tantau, 2013). For example, an inclusion of different people into new product development can result not only in a number of actual new ideas and perspectives but bear the danger of involuntary knowledge leakage as well (Durst, Aggestam et al.,). The more potential partners the company cooperates with, the higher the relational risks resulting from this cooperation.

15. Knowledge outsourcing risks

Outsourcing can be defined as transferring a business activity or function from a company to an external contractor who takes control of the activity's inputs and then performs that function, selling it back to the company (Tadelis, 2007). The outsourcing of business activities/functions also involves a number of knowledge risks such as a risk of losing skills and capacities that are needed to perform central (knowledge) processes (Agndal & Nordin, 2009). Furthermore, too strong an identification with a client organization can hamper the success of outsourcing activities and undermine KM practices in the originating organization (Edvardsson & Durst, 2014). Referring to knowledge risks, relying on external contractors for risk management may lead to an overemphasis of minor knowledge risks and an underestimation of major ones.

16. Risk of using obsolete/unreliable knowledge

Knowledge may quickly become obsolete or irrelevant (Tan et al., 2006). Therefore, it should be continuously updated and refreshed. If a company does not keep its knowledge up-to-date or validated, there is a risk that it will apply wrong knowledge in its operations. This may take place in two situations: 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 & Durst, 2018). Such situations bring negative consequences, as they jeopardize the reliability of the company and may lead to various types of losses (e.g. losses of financial resources, reputation, customers, partners, etc.).

17. Risk of improper knowledge application

Another risk that organizations face nowadays is a risk of improper application of knowledge or its misinterpretation. For example, a company might obtain knowledge about a certain business opportunity, but due to the lack of abilities and skills to critically analyze it, the company might misinterpret it and make the wrong decision (Zieba & Durst, 2018). Proper knowledge usage is a challenge for organizations, as the amounts of available knowledge are enormous and therefore, applying all this knowledge requires skills and competencies.

18. Espionage

Merriam-Webster Dictionary defined espionage as "the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company". Industrial espionage is essentially a sort of commercial intelligence gathering, often by industry competitors (Crane, 2005). In the era of global competition, companies are forced to gather information about their competitors, their products, and activities. However, there is a point when industrial espionage becomes an unethical practice. According to Crane (2005), such a situation takes place when one of the following incidents happens:

(1) The tactics applied to secure information are questionable (i.e. they go beyond what might be perceived as acceptable, ethical, or legal business practice).
(2) The nature of the collected information is in some way private or confidential.
(3) The aim for which the information is used is against the public interest.

According to Chan (2003), the consequences of industrial espionage are severe to organizations not only with regard to financial aspects but also with regard to other areas of company's operations. Growing corporate espionage actions often cause the introduction of highly controlling security measures and intensive employee monitoring. All this brings distrust to organizations. Therefore, industrial espionage is linked not only to knowledge loss but also to the loss of open culture, based on knowledge exchange and trust.

19. Continuity risks

According to Lambe (2013), these risks 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. Thus, in order to address the likely risks organizations of any kind should have a decent approach to succession planning/people replacement in place (Durst & Wilhelm, 2012). The reality, however, shows that despite the many awareness-raising activities conducted at regional, national and international levels, succession planning continues to be a neglected activity in organizations (Durst & Bruns, 2016) which in turn increases the likelihood of making this category of risks a permanent one.

20. Communication risks

According to Merriam Webster dictionary, communication can be defined as a process by which information is exchanged between individuals through a common system of symbols, signs, or behavior. In the context of learning and knowledge management, communication is critical as it will be needed to make knowledge practices possible. We also know that communication is exposed to noise which refers to anything that interferes with the communication process between a speaker and an audience. For example, a workshop intended to inform the audience about a new work method for a specific process will be heavily affected by participants who are mainly drawn to their smartphones or by interruptions such as ringing smartphones or the sounds of the streets. All these interferences bear the risks that the intended message is not received, partially received, received but not understood or sent differently because of the broken communication flow.

21. Knowledge acquisition risks

Knowledge acquisition risks relate to an organization's ability to acquire the new knowledge it needs in order to follow a new strategic direction (Lambe, 2013). New knowledge is needed in different situations such as for innovation in general or continued skill and competence development to make sure that organizations are able to weather present and future business challenges. This activity – which should be deeply embedded in organizations – may increase the risks that wrong knowledge is acquired, or the knowledge is acquired only partially (e.g. just the explicit knowledge elements are acquired). Thus, this type of risk is closely linked with the risks of using obsolete/unreliable knowledge and that of applying knowledge improperly as presented before.

22. Knowledge transfer risks

According to Argote and Ingram (2000), knowledge transfer in organizations "is the process through which one unit (e.g., group, department, or division) is affected by the experience of another" (p. 151) and incorporates the idea of knowledge exchanged in return for some other asset (or for other knowledge). Focusing on knowledge transfer as a people-to-people process (Tangaraja, Rasdi, Samah, & Ismail, 2016), the successful transfer of knowledge may be hampered by a number of factors which can be assigned to personal factors (e.g. motivation, trust, relational competencies, absorptive capacities, common language), organizational factors (e.g. culture, commitment of management to make available resources and time, incentives provided, context) and the nature of the knowledge in question (explicit versus tacit knowledge, stickiness) (Alavi & Leidner, 2001; Cohen & Levinthal, 1990; Davenport & Prusak, 1998; Fong & Lee, 2009;

Geisler, 2007; Hislop, 2009; Szulanski, 1996; Van Zolingen, Streumer, & Stooker, 2001). Flawed knowledge transfer will also increase the emergence of a number of other knowledge risks as presented in this paper.

23. Merger & acquisition (M&A) risks

In the context of mergers and acquisitions, several knowledge risks can occur. First, proper communication may be missing, which can lead to misunderstandings and a lack of knowledge exchange. Second, knowledge retention can be an issue, as, often, in mergers and acquisitions, the number of staff is reduced which, in turn, can contribute to the attrition of crucial knowledge. Third, there could be a problem with regard to the availability of knowledge in the newly created organization. With the new organizational structure, knowledge can be stuck somewhere and not available where it is really needed.

Integrations risks can be considered as a sub-form of M&A risks as 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 way so that it is usable for the members of the newly formed organization. This integration may be hampered by the existence of different cultures, contexts but also different mindsets, worldviews, values of the actors involved. In such an environment, critical knowledge in the form of skills or capacities might be lost or neglected which in turn is likely to lead to the execution of tasks and processes which are sub-optimal or in the worst case no longer executable. Thus, integration risk refers to the missing fit of strategic, operational, behavioral and cultural aspects in the newly created organization (Cartwright & Schoenberg, 2006).

24. Outcomes of knowledge risks

All the above-mentioned knowledge risks are potential hazards to organizations, although their appearance or consequences are diversified (i.e. not of the same kind to all types of organizations). These knowledge risks may bring about various consequences, such as knowledge attrition, knowledge loss, knowledge leakage or lost reputation. All the identified potential outcomes are briefly presented and described in Table 1.

Knowledge risks identified in the previous sections together with their potential consequences need to be classified and organized for better clarity and overall understanding. Thus, in the next section, it is aimed to place these risks and their outcomes in a sort of order by presenting them in a form of taxonomy (a concept map).

25. Development of knowledge risk taxonomy

The term "taxonomy" means "the rules or conventions of order or arrangement" (Lambe, 2007, p. 4). It comes from the Greek *taxis* = ordering and *nomos* = law, norm, rule (Currás, 2010, p. 37) and was coined by De Candolle in 1813 for the purpose of designing the rules or laws to be used in systematics (Currás, 2010). The use of taxonomy in its classic form was limited to biology and logic, but presently it has been extended to other fields, e.g. information science (Currás, 2010).

Taxonomies can be visually presented in a variety of forms (Lambe, 2007). Among them are lists, trees, hierarchies, polyhierarchies, matrices, facets, or systems maps. All these forms are valid ways of presenting taxonomies and the actual choice depends on the value and function. The crucial condition is to help users understand and navigate the structure of the subjects depicted in the taxonomy (Lambe, 2007).

For the purpose of this paper, the authors decided to use a concept map. Concept mapping is a generic term that describes any process for representing ideas in pictures or maps (Kane & Trochim, 2007). Concept maps are useful for cataloging specialist knowledge domains and explaining them in an easily accessible way (Lambe, 2007). Concept sorting is a simple, but powerful, approach for generating, sorting, arranging and rearranging any set of elements (e.g., ideas or concepts) in a visually explicit manner – a concept map (Lawless, Smee, & O'Shea, 1998). The form of concept mapping that the authors applied is in accordance with the proposal of Novak and Gowin (1984). Thus, the authors produced a picture of all knowledge risks and established the relationships between them. Next, the possible consequences of these knowledge risks (e.g., lost reputation) were added. The resulting map presents each idea (i.e., each knowledge risk) in a separate oval with lines connecting related ideas (Jackson & Trochim, 2002).

Following the specification of the knowledge risks presented before, the authors of this paper propose a concept map of knowledge risks. This map is depicted in Figure 1.

26. Approaches and tools to manage knowledge risks

The plethora of potential knowledge risks that may occur in organizations requires a set of tools and approaches intended to identify, prevent or manage them. For example, knowledge maps, in general, locate important knowledge in organizations and provide information on where to find it (Davenport & Prusak, 1998). Thus, with the aid of these maps strategic knowledge assets could be identified. The identification

Table 1. Consequences of knowledge risks.

Consequences	Definition
Knowledge attrition	A process where knowledge is becoming obsolete (e.g., due to new inventions, progress in the state-of-the-art, becoming of historical value only, etc.) or corrupted (e.g., caused by inappropriate use or waiting too long to use the knowledge, etc.) (Durst & Zieba, 2017).
Knowledge loss	A situation when an organization loses a part or all of its crucial knowledge as a consequence of for example employee leaving a company, employee poaching or some technical faults (e.g. computer breakdown).
Knowledge leakage	A situation "when sensitive organizational knowledge such as strategies, policies, product knowledge, and sensitive client information ends up in the hands of unauthorized parties" (Ahmad, Bosua, & Scheepers, 2014, p. 28).
Knowledge spillover	A situation when valuable knowledge spills out of the organisation to competitors who use this knowledge to gain competitive advantage (Durst & Zieba, 2017).
Lost reputation	A situation when a company loses "the observers' collective judgments based on assessments of financial, social and environmental impacts attributed to the company over time" (Financial Times Lexicon, 2017).
Lost sustainability	A situation when a company loses its ecologically-balanced approach towards the operations and does not follow the rules of sustainable development any more. (Financial Times Lexicon, 2017).

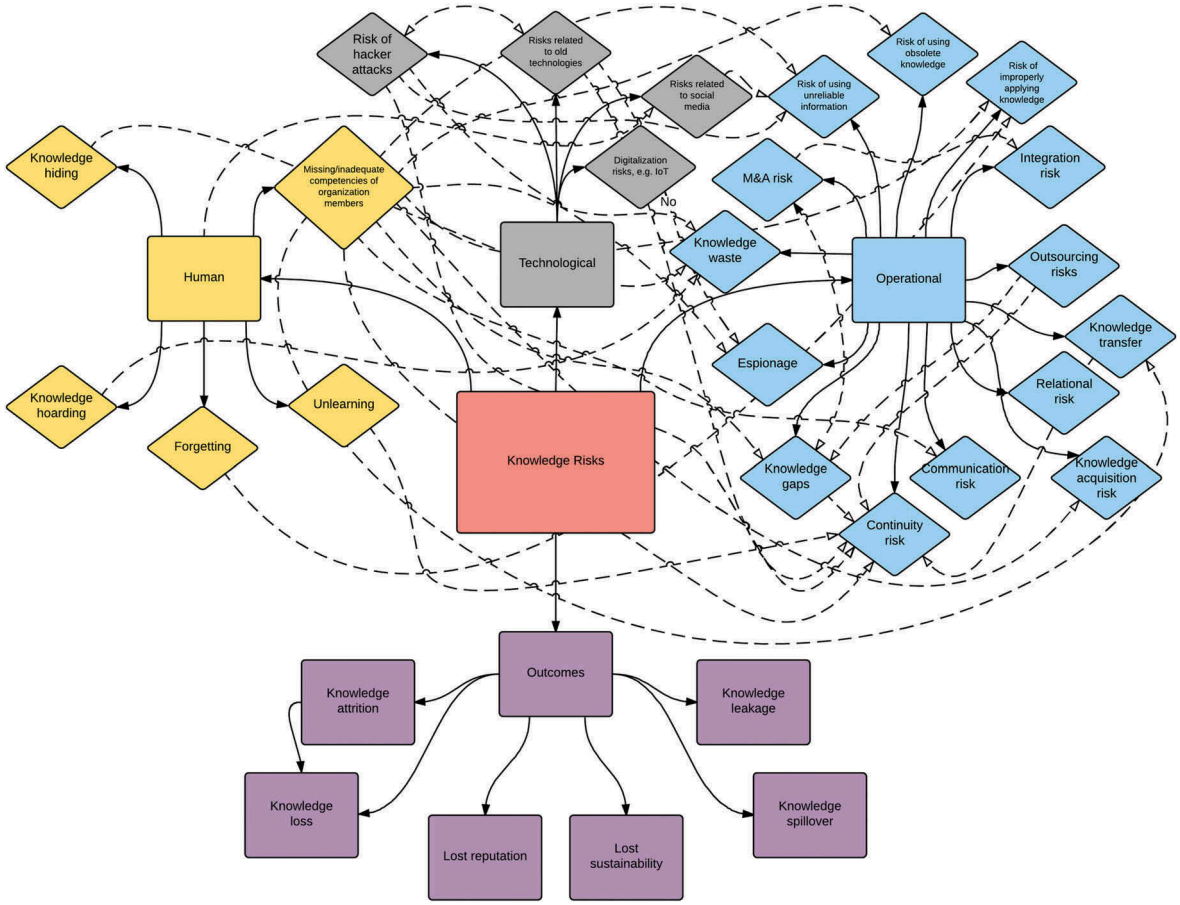

Figure 1. Knowledge risks map.

of strategic knowledge assets by managers or owners can be viewed as the first necessary step to address potential knowledge risks (Carlucci & Schiuma, 2006; Durst & Aisenberg Ferenhof, 2016; Marr, Neely, & Schiuma, 2004). To raise awareness about the different qualities knowledge/intellectual capital (IC) may assume in different situations, e.g., being an asset or a liability, Durst and Wilhelm (2013) developed a tool intended to provide a better understanding of the likely dependency on certain organization members. To do so, the tool calculates a so-called "knowledge at risk"-scale. This scale represents the sum of four dimensions respectively values which are human capital, structural capital, relational capital and social capital. The tool consists of various levels, which need to be filled and can be adjusted to the requirements of the organization in question. In the end, the instrument provides a report displaying the overall result ("the knowledge at risk"-score) and the results for each of the four dimensions. Based on this understanding, the organization could initiate actions aimed at managing the critical knowledge/IC in the best way possible.

Durst and Aisenberg Ferenhof (2016) have proposed a framework for knowledge risk management in small and medium-sized enterprises. According to these authors, knowledge risk management consists

of four phases: 1) knowledge risk identification, 2) qualitative and quantitative analysis of the risks identified in stage 1, 3) management and control of present and future knowledge risks, and 4) continued knowledge risk reporting.

As regards ways of protecting critical organizational knowledge, the study of Zięba (2017) shows that organizations have a number of different options at hand:

- To motivate and encourage employees to share their knowledge and not to take it away;
- To transfer and store crucial knowledge in IT-based databases;
- To share crucial knowledge only with a limited number of people/firms within and outside the organization;
- To do continued back-ups of data and databases;
- To apply solutions/tools that are sufficiently protected;
- To have installed different levels of knowledge access – i.e., only available to those persons who need such knowledge to perform their tasks.

Additionally, organizations may also:

- protect their strategic knowledge assets by legal arrangements, copyrights, etc.;
- retain critical knowledge through codification and distribution in organizations (Martins & Martins, 2011);
- eliminate redundant knowledge from their organizational memory;
- be cautious in selecting outsourcing and cooperating partners to minimize the risk of improper knowledge usage by these parties (Edvardsson & Durst, 2014; Zięba, 2017);
- implement knowledge management solutions that incorporate risk management (Durst & Aisenberg Ferenhof, 2016).

27. Discussion and conclusions

As clarified in Figure 1, there are many potential knowledge risks that contemporary organizations can face. These risks can be grouped into three categories: human knowledge risks, operational knowledge risks, and technological knowledge risks. Each category encompasses several knowledge risks, while the most abundant one is the operational knowledge risk category. This is not surprising, as many knowledge risks relate to regular, day-to-day operations of organizations. As these operations are in many cases necessary, there is a relatively high likelihood that knowledge risks will sooner or later compromise the outcome of these operations. That is why especially these knowledge risks should be analyzed and continuously monitored by organizations.

The proposed knowledge taxonomy underlines the links between the different knowledge risks which in turn requires the organization to avoid having an isolated view of certain knowledge risks but an integrated view comprising all types of knowledge risks as well as the consequences that flow from knowledge-related decisions. It has to be stressed (and clearly outlined on the map), knowledge risks should be taken seriously in the entire organizations and not be limited to the realm of certain persons/departments. If an organization aims to address potential knowledge risks in a systematic way, it needs to start with a clear strategy and then develops both a proper risk governance that comprises the needed structures and processes as well as a (knowledge) risk-aware culture. All organization members should be prepared and used to detect potential knowledge risks and, and even more important, to talk about these risks in order to reduce the extent of damage at an early stage. Having knowledge risk champions would be ideal in order for knowledge risk management/activities to flourish in the organization, taking into account the significance of these persons for organizations (Kotter, 1995). An ideal approach to knowledge risk management would be based on a concentrated approach involving people and IT measures in order to bring together the strengths of both approaches. Additionally, just focusing on people approaches is not enough, as the individual actor will be overstrained by the challenges ahead while just emphasizing IT solutions may create a false sense of security (and as outlined above may have serious consequences for organizations). The knowledge risks related to the human factor suggest that organizations should pay more attention towards culture, trust issues, and motivational aspects. Working on these three aspects could help organizations in reducing the risk of, for example, hoarding or forgetting knowledge (Alavi, Leidner, & Kayworth, 2006; Nissen, 2006). It also underlines – in conjunction with what has been discussed before – the need for training in different areas (e.g. risk management, knowledge risks particularly those related to digitalization, governance etc.).

KR and possible ways of addressing them may also be related to the type of knowledge they concern. The most prevalent way to categorize knowledge is to make it either explicit or tacit (Nonaka, 1994). Explicit knowledge is typically formal, codified, documented and available in a form that can be easily shared, while tacit knowledge cannot be effectively codified and is interlinked with individuals and their expertise. The specific type of knowledge puts an additional challenge on an organization´s ability to cope with KR and thus should be attended differently. For example, tacit

knowledge can be hoarded or forgotten, which is rarely the case with explicit knowledge.

Against the background of the knowledge risks that are related to digital transformation and a world that is increasingly computerized one should acknowledge that everything is hackable. However, this does not mean that organizations are completely helpless and unprotected. In fact, a number of companies (companies from Israel in particular, see: https://www.jpost.com/Jpost-Tech/As-hackers-gain-strength-Israeli-cyber-firms-raise-more-money-than-ever-540175) have started working on solutions for addressing these cyber challenges. The insurance industry (e.g., the German insurance company Allianz) too has expanded its portfolio and is offering an increasing number of insurance products aimed at IT and cyber risks.

28. Study implications, limitations, and further research possibilities

The implications of this study for academia and practice are multiple. First, the paper offers a better understanding of knowledge risks, their definitions, outcomes and relations to each other. Thus, it brings together a field that has been rather fragmented to date. More precisely, the paper offers a taxonomy of a plethora of knowledge risks that organizations might potentially suffer from. With the use of this taxonomy, more rigor research activities will be possible. Organizations, on the other hand, might analyze their present situation and prepare a strategy dealing with crucial knowledge risks. With the help of the taxonomy, organizations can answer the question "Where do we start?", which is a common question for implementing any KM initiative (Earl, 2001). Following the risk assessment process developed by Kaplan and Garrick (1981), which answers three major questions: "What can go wrong?", "What is the likelihood?" and "What are the consequences?", the proposed taxonomy answers the first question – what can go wrong. The next two questions can be answered with a risk management approach that also takes into account knowledge risks (Durst & Aisenberg Ferenhof, 2016). Some of the risks can be completely eliminated or minimized, while others can be anticipated to come and their impact, therefore, can be reduced.

The taxonomy of knowledge risks also makes the understanding of knowledge management more comprehensive – it is not sufficient to manage critical organizational knowledge, it is also important to understand the downsides of knowledge and protect against them. As Massingham (2010) stated, "individual response to risk depends upon whether you feel it is entirely random or can be managed" (p. 465). Managers in organizations should assume they can manage the risk by anticipating its occurrence and by initiating measures to reduce its impact. As these activities come at a cost, managers are always required to make a trade-off between risk and return. Yet, by being aware of a number of potential knowledge risks and by having tools at hand that support in managing these risks, organizations will be brought in a position to better weather the business challenges ahead.

The study has some limitations. First, as the taxonomy is of a theoretical character, it has not been examined in the practical context. Second, although the authors believe that the taxonomy is rather comprehensive, they may have overlooked some additional relevant knowledge risks that may impact organizations. Finally, as the research area is in its infancy, there are not many references we could base on.

As far as future research avenues are concerned, the taxonomy offers many possibilities. The first one would be to examine the awareness and understanding of knowledge risks in organizations, using the proposed taxonomy as a starting point. The second area of interest would be to evaluate the perceived importance of the knowledge risks presented in the taxonomy, by answering the questions:

- How relevant are these knowledge risks from an organizational perspective, different types of organizations/industries etc.?
- How do organizations manage the relevance of these risks over time?

The third possibility could be the examination of preventive actions organizations undertake to manage particular knowledge risks and the efficiency of these actions. Fourth, as managing knowledge risks in organizations will require every organization member, the following questions originate:

- how to develop a (knowledge) risk-aware culture? and
- how to make it a quick process to keep pace with the reality of knowledge risks?

Last but not least, the focus of this paper has been on knowledge risks at the organizational level, thus other levels such as individual level have not been considered but may hold a number of additional knowledge risks which should be addressed in future research.

Acknowledgments

Malgorzata Zieba gratefully acknowledges support from the National Science Centre (Poland) in the context of a research project "Knowledge management strategies and their determinants in companies from the knowledge-intensive business service sector" (No. 2016/21/B/HS4/03051).

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This work was supported by the National Science Centre (Poland); [No. 2016/21/B/HS4/03051].

ORCID

Susanne Durst http://orcid.org/0000-0001-8469-2427

References

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

Ahmad, A., Bosua, R., & Scheepers, R. (2014). Protecting organizational competitive advantage: A knowledge leakage perspective. *Computers and Security*, *42*, 27–39.

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

Alavi, M., Leidner, D. E., & Kayworth, T. R. (2006). An empirical examination of the influence of organizational culture on knowledge management practices. *Journal of Management Information Systems*, *22*(3), 191–224.

Argote, L., & Ingram, P. (2000). Knowledge transfer: A basis for competitive advantage in firms. *Organizational Behavior and Human Decision Processes*, *82*(1), 150–169.

Aula, P. (2010). Social media, reputation risk and ambient publicity management. *Strategy & Leadership*, *38*(6), 43–49.

Becker, K. (2008). Unlearning as a driver of sustainable change and innovation: Three Australian case studies. *International Journal of Technology Management*, *42*(1/2), 89–106.

Carlucci, D., & Schiuma, G. (2006). Knowledge asset value spiral: Linking knowledge assets to company's performance. *Knowledge and Process Management*, *13*(1), 35–46.

Cartwright, S., & Schoenberg, R. (2006). Thirty years of mergers and acquisitions research: Recent advances and future opportunities. *British Journal of Management*, *17*, S1–S5.

Černe, M., Hernaus, T., Dysvik, A., & Škerlavaj, M. (2017). The role of multilevel synergistic interplay among team mastery climate, knowledge hiding, and job characteristics in stimulating innovative work behavior. *Human Resource Management Journal*, *27*(2), 281–299.

Cerne, M., Nerstad, C. G. L., Dysvik, A., & Skerlavaj, M. (2014). What goes around comes around: Knowledge hiding, perceived motivational climate, and creativity. *Academy of Management Journal*, *57*(1), 172–192.

Chan, M. (2003). Corporate espionage and workplace trust/distrust. *Journal of Business Ethics*, *42*(1), 45–58.

Chatzoudes, D., Chatzoglou, P., & Vraimaki, E. (2015). The central role of knowledge management in business operations: Developing a new conceptual framework. *Business Process Management Journal*, *21*(5), 1117–1139.

Cohen, W. M., & Levinthal, D. A. (1990). Absorptive capacity: A new perspective on learning and innovation. *Administrative Science Quarterly*, *35*(1), 128–152.

Connelly, C. E., & Zweig, D. (2014). How perpetrators and targets construe knowledge hiding in organizations. *European Journal of Work and Organizational Psychology*, *24*(3), 479–489.

Connelly, C. E., Zweig, D., Webster, J., & Trougakos, J. P. (2012). Knowledge hiding in organizations. *Journal of Organizational Behavior*, *33*, 64–88.

Coras, E. L., & Tantau, A. D. (2013). A risk mitigation model in SME´s open innovation projects. *Management & Marketing Challenges for the Knowledge Society*, *8*(2), 303–328.

Crane, A. (2005). In the company of spies: When competitive intelligence gathering becomes industrial espionage. *Business Horizons*, *48*(3), 233–240.

Currás, E. (2010). *Ontologies, taxonomies and thesauri in systems science and systematics. Ontologies, taxonomies and thesauri in systems science and systematics*. Oxford, UK: Chandos Publishing.

Davenport, T. H., & Prusak, L. (1998). *Working knowledge. How organizations manage what they know*. Boston, Massachusetts: Harvard Business School Press.

De Holan, P. M. (2011). Agency in voluntary organizational forgetting. *Journal of Management Inquiry*, *20*(3), 317–322.

Delerue, H. (2005). Relational risk perception and alliance management in French biotechnology SMEs. *European Business Review*, *17*(6), 532–546.

Durst, S. (2012). Innovation and intellectual capital (risk) management in small and medium-sized enterprises. *International Journal Transitions and Innovation Systems*, *2*(3/4), 233–246.

Durst, S., & Aisenberg Ferenhof, H. (2016). Competitive strategies for small and medium enterprises knowledge risk management in turbulent times. In K. North & G. Varvakis (Eds.), *Competitive strategies for small and medium enterprises* (pp. 195–209). Cham: Springer International Publishing.

Durst, S., Aggestam, L., & Aisenberg Ferenhof, H. (2015). Understanding knowledge leakage: A review of previous studies. *VINE Journal of Information and Knowledge Management System*, *45*(4), 568–586.

Durst, S., & Bruns, G. (2016). Sustaining the future of the public sector: Insights into a swedish municipality's dealing with knowledge management and succession planning. *Journal of Information & Knowledge Management*, *15*(Iss), 2.

Durst, S., & Wilhelm, S. (2011). Knowledge management in practice: Insights into a medium-sized enterprise's exposure to knowledge loss. *Prometheus*, *29*(1), 23–38.

Durst, S., & Wilhelm, S. (2012). Knowledge management and succession planning in SMEs. *Journal of Knowledge Management*, *16*(4), 637–649.

Durst, S., & Wilhelm, S. (2013). Do you know your knowledge at risk? *Measuring Business Excellence*, *17*(3), 28–39.

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

Earl, M. J. (2001). Knowledge management strategies: Toward a taxonomy. *Journal of Management Information Systems*, *18*(1), 215–233.

Edvardsson, I. R., & Durst, S. (2014). Outsourcing of knowledge processes: A literature review. *Journal of Knowledge Management*, *18*(4), 795–811.

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.
Financial Times Lexicon. Retrieved September 27, 2017, from. http://lexicon.ft.com/Term?term=corporate-reputation&mhq5j=e7
Fong, P. S. W., & Lee, H. F. (2009). Acquisition, reuse and sharing of knowledge in property management firms. *Facilities*, *27*(7), 291–314.
Gartner (2018). IT Glossary. Retrieved from http://www.gartner.com/it-glossary/digitalization/
Geisler, E. (2007). The metrics of knowledge: Mechanisms for preserving the value of managerial knowledge. *Business Horizons*, *50*, 467–477.
Haimes, Y. Y. (2009). On the complex definition of risk: A systems-based approach. *Risk Analysis*, *29*(12), 1647–1654.
Hislop, D. (2009). *Knowledge management in organizations: A critical introduction* (2nd ed.). Oxford: Oxford University Press.
Holten, A. L., Hancock, G. R., Persson, R., Hansen, Å. M., & Hogh, A. (2016). Knowledge hoarding: Antecedent or consequent of negative acts? The mediating role of trust and justice. *Journal of Knowledge Management*, *20*(2), 215–229.
Jackson, K. M., & Trochim, W. M. K. (2002). Concept mapping as an alternative approach for the analysis of open-ended survey responses. *Organizational Research Methods*, *5*(4), 307–336.
Kane, M., & Trochim, W. M. K. (2007). *Concept mapping for planning and evaluation* (Vol. 50). USA: Sage Publications. doi:10.4135/9781412983730
Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Analysis*, *1*(1), 11–27.
Kotter, J. P. (1995, March-April). Leading change: Why transformation efforts fail. *Harvard Business Review*, 59–67.
Lambe, P. (2007). *Organising knowledge: Taxonomies, knowledge and organisational effectiveness*. Oxford, England: Chandos Publishing.
Lambe, P. (2013), Four types of knowledge risk, Retrieved April 03, 2017, from. http://www.greenchameleon.com/uploads/Four_Types_of_Knowledge_Risk.pdf
Lawless, C., Smee, P., & O'Shea, T. (1998). Using concept sorting and concept mapping in business and public administration, and in education: An overview. *Educational Research*, *40*(2), 219–235.
Lee, L. T.-S., & Sukoco, B. M. (2011). Reflexivity, stress, and unlearning in the new product development team: The moderating effect of procedural justice. *R&D Management*, *41*(4), 410–423.
Lee, S., Suh, E., & Lee, M. (2014). Measuring the risk of knowledge drain in communities of practice. *Journal of Knowledge Management*, *18*(2), 382–395.
Lei, D., Slocum, J. W., & Pitts, R. A. (Winter, 1999). Designing organizations for competitive advantage: The power of unlearning and learning. *Organizational Dynamics*, *27*(3), 24–38.
Leonard, D. (2014), How to prevent experts from hoarding knowledge. *Harvard Business Review*. Retrieved from https://hbr.org/2014/12/how-to-prevent-experts-from-hoarding-knowledge
Marr, B., Neely, A., & Schiuma, G. (2004). The dynamics of value creation: Mapping your intellectual performance drivers. *Journal of Intellectual Capital*, *5*(2), 312–325.
Martins, E., & Martins, N. (2011). The role of organisational factors in combating tacit knowledge loss in organisations. *Southern African Business Review*, *15*(1), 49–69.
Massingham, P. (2008). Measuring the impact of knowledge loss: More than ripples on a pond? *Management Learning*, *39*(5), 541–560.
Massingham, P. (2010). Knowledge risk management: A framework. *Journal of Knowledge Management*, *14*(3), 464–485.
McAdam, R. (2000). Knowledge management as a catalyst for innovation within organizations: A qualitative study. *Knowledge and Process Management*, *7*(4), 233–241.
Mohamed, S., Mynors, D., Andrew, G., Chan, P., Coles, R., & Walsh, K. (2007). Unearthing key drivers of knowledge leakage. *International Journal of Knowledge Management Studies*, *1*(3–4), 456–470.
Nissen, M. E. (2006). *Harnessing knowledge dynamics: Principled organizational knowing & learning*. Hershey, USA: IRM Press.
Nonaka, I. (1994). A dynamic theory of organizational knowledge creation. *Organization Science*, *5*(1), 14–37.
Novak, J. D., & Gowin, B. D. (1984). *Learning how to learn*. Cambridge: Cambridge University Press.
Perlroth, N., Scott, M., & Frenkel, S. (2017). Cyberattack hits Ukraine then spreads internationally. *The New York Times* Retrieved June 27, 2017, October 05, 2017 from. https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html
Perrott, B. E. (2007). A strategic risk approach to knowledge management. *Business Horizons*, *50*(6), 523–533.
Polsat News. Retrieved June 12, 2018, from. http://www.polsatnews.pl/wiadomosc/2017-02-28/niemal-tysiac-oszukanych-w-falszywym-konkursie-wygrali-pobyt-w-hotelu-w-karpaczu/.
PWC. (2016). *Directors and IT A user-friendly board guide for effective information technology oversight (abridged version)*.
Stam, C. D. (2009). Intellectual liabilities: Lessons from the decline and fall of the Roman Empire. *The Journal of Information and Knowledge Management Systems*, *39*(1), 92–104.
Szulanski, G. (1996). Exploring internal stickiness: Impediments to the transfer of best practice within the firm. *Strategic Management Journal*, *17*, 27–44.
Tadelis, S. (2007). The innovative organization: Creating value through outsourcing. *Californian Management Review*, *50*(1), 261–277.
Tan, H. C., Carrillo, P., Anumba, C., Kamara, J. M., Bouchlaghem, D., & Udeaja, C. (2006). Live capture and reuse of project knowledge in construction organisations. *Knowledge Management Research & Practice*, *4*, 149–161.
Tangaraja, G., Rasdi, R. M., Samah, B. A., & Ismail, M. (2016). Knowledge sharing is knowledge transfer: A misconception in the literature. *Journal of Knowledge Management*, *20*(4), 653–670.
Techopedia. Retrieved September 24 2017, from. https://www.techopedia.com/definition/2387/cybercrime
The Economist. (2017). *Why everything is hackable*, April 8th 2017, 69–71.
Tsang, E. W. K., & Zahra, S. A. (2008). Organizational unlearning. *Human Relations*, *6*(10), 1435–1462.
Van Zolingen, S. J., Streumer, J. N., & Stooker, M. (2001). Problems in knowledge management: A case study of a knowledge-intensive company. *International Journal of Training and Development*, *5*(3), 168–184.

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* (8), 1–37.

Why knowledge transfer needs to start long before retirement? Retrieved September 14 2017, from. http://adigaskell.org/2015/01/02/why-knowledge-transfer-needs-to-start-long-before-retirement/

Zahra, S. A., Abdelgawad, S. G., & Tsang, E. W. K. (2011). Emerging multinationals venturing into developed economies: Implications for learning, unlearning, and entrepreneurial capability. *Journal of Management Inquiry*, *20*(3), 323–330.

Zieba, M., & Durst, S. (2018). Knowledge Risks in the Sharing Economy. E.-M. Vătămănescu & F. Pînzaru, Eds., *Knowledge management in the sharing economy* (pp. 253–270). Cross-Sectoral Insights into the Future of Competitive Advantage, Springer.

Zięba, M. (2017). Knowledge safety – Insights from the SME sector. *Journal of Management and Business Administration. Central Europe*, *25*(3), 78–96.