„Journal of Management and Business Administration. Central Europe"
Vol. 25, No. 3/2017, p. 78–96, ISSN 2450-7814; e-ISSN 2450-8829

Knowledge Safety – Insights from the SME Sector

Małgorzata Zięba[1]

Submitted: 08.12.16. Final acceptance: 02.06.17

Abstract

Purpose: This paper aims to explore the topic of knowledge safety, defined as the state of knowledge being safe from loss, *leakage, attrition, oblivion, waste or theft*. The paper first presents a theoretical background and review of previous studies on knowledge loss and ways of overcoming it, and then illustrates the topic of knowledge safety with ten case studies from the small and medium-sized enterprises (SMEs) sector.

Methodology: The paper is based on an analysis of Knowledge Management (KM) literature devoted to knowledge loss and its potential types in companies, and on the results of case study research. Knowledge safety was first defined and contrasted with other terms, and then examined in 10 selected SMEs. The research resulted in a clarification of what SMEs understand by the term of "*knowledge safety*" and what kind of measures they take to ensure it.

Findings: As the analysis shows, the examined SMEs attribute diversified significance to the issue of knowledge safety. For some of them, such problem does not exist at all and they state that they can ensure knowledge safety in all aspects of their operations. Some companies perceive it mainly through the safety of the knowledge stored in electronic databases, while others link it with the human factor only.

Research limitations: Research results are limited to ten companies operating in Poland. As such, they cannot illustrate the whole picture of the existing small or medium-sized companies.

Research implications: The findings of both literature review and case study analysis indicate that there is a need to further examine the issue of knowledge safety by analysing the potential factors which may endanger knowledge safety and the methods to eliminate such risks.

Practical implications: The paper examines important aspects of knowledge safety and provides guidelines on how it can be ensured by managers or owners of SMEs.

Originality/value: The term of knowledge safety has been absent from the related literature so far. The paper defines it and explores both the theoretical and the practical aspects thereof. The paper also suggests further research possibilities in this area.

Keywords: knowledge safety, knowledge loss, small and medium-sized enterprises, case study

JEL: M10

[1] Gdansk University of Technology
Correspondence address: Gdansk University of Technology, Faculty of Management and Economics, 11/12 Narutowicza St., 80-233 Gdansk, email: mz@zie.pg.gda.pl.

Ministry of Science and Higher Education Republic of Poland

English-language editing of that article was financed under Agreement 763/ P-DUN /2016 with funds from the Ministry of Science and Higher Education allocated to the popularization of science.

Introduction

Knowledge is becoming an increasingly significant asset of contemporary organizations. It is therefore not surprising that companies search for new, more efficient ways of managing their knowledge and pay a growing attention to knowledge management (KM) techniques and methods. There is a specific situation taking place in small and medium-sized companies, where KM is often of informal, emergent character (Zieba et al., 2016). Additionally, many knowledge-related activities and processes in such companies, such as e.g. systematic, formal documentation, are simply absent (Shelton, 2001). As earlier studies show, even if SMEs are aware of the importance of their knowledge assets, they generally tend to follow an unplanned, unsystematic, and informal approach to managing their knowledge (Edvardsson, 2006; 2009; Hutchinson and Quintas, 2008). Knowledge can be understood in a variety of ways and its definition is often provided in the context of data and information. There is no consensus among researchers on a single, unified approach towards these three terms. For example, Awad and Ghaziri (2004) define data as "a set of discrete facts about events – structured records of transactions", information as "an aggregation of data that makes decision making easier and consists of facts and figures based on reformatted or processed data", while knowledge is considered as "human understanding of a specialized field of interest that has been acquired through study and expertise". As it can be seen, data, information, and knowledge are all interlinked, and data can be transformed into information and information into knowledge. For the purpose of this paper, the author uses the definition of knowledge provided by Holsapple (2003), who defined knowledge as a "combination of information, ideas, experience and insights that guide actions and decisions". In the opinion of the author, this definition illustrates the sense of knowledge in organizations well, as it highlights the purpose of possessing knowledge – to help organizations in undertaking actions and making decisions. There is a particular need to deal with knowledge and its safety in organizations, as many organizations concentrate only on their data and information while neglecting knowledge in this context. For example, data and information stored in IT solutions is often secured in a certain way, such as a back-up copy or passwords, and knowledge is more difficult to be protected using some formal mechanisms.

For many companies from the SME sector, reliance on tacit, not documented knowledge makes them highly vulnerable to a loss of key employees and key knowledge. In a pessimistic scenario, the loss of a single key employee and their knowledge might result in the threat of the company's going out of business (Durst and Wilhelm, 2011). Apart from losing an employee and their knowledge, companies might also lose crucial knowledge in a variety of other ways, e.g. by knowledge leakage, knowledge waste, or

DOI: 10.7206/jmba.ce.2450-7814.203

knowledge theft. At the same time, the decision on whether and to what extent knowledge should be retained or protected depends on the awareness of the risk of losing knowledge and the significance of the problem it might cause (Levy, 2011). This awareness might be not high among SME managers, who generally tend to focus on daily problems instead of anticipating future problems.

As it has been reported in some studies, organizations have to face a growing wave of knowledge loss and attrition due to layoffs, retirements, mergers, and acquisitions (Martins and Martins, 2011), as well as more competitive recruiting, faster turnover among young people, and ageing workforce (De Long and Davenport, 2003). As loss of knowledge can result in many negative consequences for organizations, such as disrupted operations, reduced efficiency, sales and product/service quality (Eckardt et al., 2014), organizations should pay attention to knowledge retention and concentrate on ensuring safety of their crucial knowledge.

Taking the above into account, there is a need to introduce a new concept of knowledge safety. On the basis of literature analysis it can be concluded that the knowledge possessed by SMEs can be exposed to loss or attrition and has to be managed or retained to prevent these phenomena from occurring. Therefore, the following questions arise:

> "How do organizations understand knowledge safety? What kind of potential hazards endangering their knowledge safety do they identify? What kind of actions do they undertake on everyday basis to provide knowledge safety?"

This paper aims to answer these questions by presenting results of an empirical investigation involving 10 owners and managers of small and medium sized companies located in one of the regions of Poland. The research utilizes a case study method and gives grounds for a preliminary analysis of the concept of knowledge safety.

The paper is structured as follows. The next section presents a brief review of the literature on knowledge loss and knowledge retention/protection in SMEs, and also offers the concept of knowledge safety. The third section describes the applied research methodology and the research questions. Section four presents the main findings of the empirical investigation, while the last two sections discuss and summarize the main results, and illustrate the possible implications for research and management.

Literature review

Knowledge loss

Knowledge loss has become a challenge to organisations that wish to remain competitive (Martins and Martins, 2011). At the same time, the scale of problems related to knowledge loss is increasing due to three phenomena: 1. Knowledge itself is becoming a critical organizational resource; 2. Employee turnover rates are increasing and, in many cases, employees are not replaced by new ones; 3. The average age of the labour force is growing, posing a potential hazard of many retirees in the years to come (Massingham, 2008).

There can be several potential reasons for the knowledge loss identified. The most obvious one is employee turnover, either voluntary (i.e. when an employee resigns or retires) or involuntary (when an employee is dismissed) (Shaw et al., 1998). In the case of SMEs, even short or long term periods of employee absence may lead to substantial threats due to difficulties with employee substitution (Durst and Wilhelm, 2011). An even more serious reason for knowledge loss can be employee poaching, when employees are enticed and "stolen" by another organization, often a competitor. In such a case, the knowledge that is lost might be of particular importance and its lack can have severe consequences. Many small enterprises are even reluctant to invest in workforce skills development, keeping in mind the risk of skilled labour being "poached" by other, often larger organisations offering usually more attractive salaries and promotional opportunities (Panagiotakopoulos, 2012).

Among other situations when organizational knowledge is lost, one can list: knowledge leakage, knowledge spillover, knowledge theft, knowledge forgetting, knowledge unlearning, and knowledge waste. Knowledge leakage takes place "when sensitive organizational knowledge such as strategies, policies, product knowledge, and sensitive client information ends up in the hands of unauthorized parties" (Ahmad et al., 2014, p. 28). In this sense, it is a type of knowledge loss since in its consequence, a company loses the uniqueness of its knowledge and, potentially, also its competitive advantage. Knowledge leakage can be intentional (e.g. when a former employee reveals some sensitive knowledge to the company's competitors) or unintentional (e.g. when an employee makes a mistake and sends some part of knowledge to unauthorized parties).

Another type of knowledge loss is knowledge spillover. It can be defined as a situation when valuable knowledge spills out of an organization to competitors, who then use this knowledge to gain competitive advantage (Durst and Zieba, 2017). Knowledge

DOI: 10.7206/jmba.ce.2450-7814.203

spillover can be beneficial to organizations if they benefit from spilled knowledge, but it can also be harmful when they lose their competitive advantage built previously on the spilled knowledge. Similarly to knowledge leakage, it can be intentional or unintentional in its character.

Knowledge theft is a special type of knowledge loss in the meaning that it is illegal and the party that steals knowledge is sought after and tried by legal authorities. Knowledge theft is a criminal offence and should not be taken advantage of by competitors to gain knowledge. Many companies may assume that they can protect their knowledge via patents, trademarks, copyrights, and so on. However, not all of the possessed knowledge can be defined according to property laws and property rights and, therefore, protected under formal mechanisms (Liebeskind, 1996).

Knowledge forgetting can be of two types: accidental and deliberate (de Holan and Phillips, 2004). An example of accidental forgetting is memory loss, i.e. a form of forgetting that is typical when knowledge is used infrequently. Deliberate forgetting takes place when some knowledge is not being taken advantage of by an organization and is consciously substituted with new knowledge. A solid differentiation between deliberate and accidental forgetting is provided by Cegarra-Navarro et al. (2013): "While accidental forgetting sees unwanted forgetting as a degradation of the stocks of organizational knowledge (e.g. accidental loss of documents on a computer by human error or mechanical breakdown, failure to preserve adequate documentation in order to interpret reports or sensor readings, etc.), intentional forgetting requires that certain routines, rules, tasks, roles, policies, values and strategies need to be actively and intentionally forgotten before new organizational knowledge can be acquired and assimilated".

Then, there is knowledge unlearning, somewhat related to deliberate knowledge forgetting. As Rebernik and Širec (2007) stated, "for unlearning to take place, intentional forgetting of some parts of existing individual and organizational knowledge is needed. Firms must "disorganize" some part of their knowledge store. Similar disorganization must also take place at individual level". In some situations, organizations need to eliminate the existing knowledge or knowledge structures to be able to explore new knowledge or to utilize their knowledge structures learned, and then knowledge unlearning is actually necessary (Cegarra-Navarro et al., 2011).

Knowledge waste takes place when an organization does not make use of the available and potentially useful knowledge. In other words, knowledge is wasted when it is available in an organization and the organization could make use of it to gain some advantage (e.g. save time, money, effort, etc.), but it does not do so (Durst and Zieba,

2017). Therefore, knowledge waste is linked with failing to make the most of the available knowledge capacity, and it can manifest itself in different ways: reinvention, lack of system discipline, underutilized human resources, scatter, hand-off, or wishful thinking (Ferenhof et al., 2015).

The consequences of knowledge loss can be of financial and non-financial character, depending on the kind of knowledge that has been lost and the way in which it has happened. For example, an obvious financial cost of losing an employee will be connected with hiring a new one (i.e. cost of the recruiting process). Also, a sudden lack of a staff member may lead to a decrease in productivity, and even to work stoppage. Financial consequences can also come from fines for improper delivery of orders. On the other hand, non-financial costs, although more difficult to be estimated, can be severe as well. Loss of a critical employee may lead to considerable gaps in the firm's intellectual capital (Durst and Wilhelm, 2011). Massingham (2008) claims that four different types of intellectual capital can be lost in such a situation: human capital, social capital, structural capital, and relational capital. For example, when an employee leaves, not only all their knowledge exits, but also their specific functional expertise, experience, skills, and contacts disappear. Structural capital supports an organization and its members in learning, while relational capital is built through an organization's relationship with the people it does business with (Stewart, 1998). When an employee leaves a firm, their knowledge on the relationships with customers, suppliers, stakeholders, and strategic alliance partners can be lost as well (Pablos, 2002).

As far as the consequences of other types of risk related to knowledge loss are concerned, they are diversified. For example, the results of knowledge leakage and knowledge spillover are related to loss of knowledge that is in many cases used by other companies, especially competitors. This can lead to a loss of competitive advantage because in order for knowledge to be a source of competitive advantage, it needs to be rare and inimitable. When it leaks out or spills over, it is not such any more. The consequences of knowledge leakage or knowledge spillover are quite difficult to be evaluated as they are of non-material character. What needs to be kept in mind is that knowledge leakage and spillover can be beneficial for a company when it is the knowledge of competitors that becomes available and a given company may then improve its competitive advantage on this basis (Mohamed et al., 2007).

In the case of knowledge theft, the consequences are of similar character to the ones resulting from knowledge leakage and spillover (i.e. the loss of important knowledge and the resulting loss of competitive advantage), but in addition to that, a company may lose its time and resources for police inquiries and judicial acts. If knowledge

DOI: 10.7206/jmba.ce.2450-7814.203

about customers is stolen, it may also affect customers' trust and, in consequence, their loyalty.

Knowledge forgetting and knowledge unlearning can actually bring positive results if they help companies and their members address new ideas, approaches, strategies (Markoczy, 1994; Gharajedaghi, 2007). However, when unlearning stops a company from conducting its operations due to a limitation of the original knowledge base, it becomes then a negative phenomenon (Wensley and Navarro, 2015). Also, forgetting can be negative when it leads to situations when an organization's staff needs to restore any previously possessed knowledge and the organization faces disruptions and/or flawed workflows (Tukel et al., 2008). Knowledge waste can bring negative consequences in the form of a loss of time on reinventing the already invented solutions and a loss of opportunities built upon the existing yet unexplored knowledge.

Both types of consequences (financial and non-financial ones) are potentially more severe for small and medium sized companies, where resources are limited and therefore, losing them and filling the missing gap is more troublesome. For example, as key staff members possess rare or difficult-to-imitate knowledge, which makes them crucial for the organization's success, determining what could potentially happen when such valuable employees leave may help an organization in evaluating the impact of knowledge loss and formulating appropriate preventive measures (Massingham, 2008). As far as other types of knowledge loss are concerned, organizations need to analyse the probability of their occurrence and the potential costs related to losing particular types of knowledge in certain ways. For example, if there is a high risk of knowledge leakage and the costs of this leakage would be severe, the company needs to identify and apply measures to prevent it (e.g. loyalty agreements with employees, careful choice of networking partners, etc.). In other words, it is crucial to identify where the loss of knowledge can have an immediate threatening effect on the organization (Martins and Martins, 2011) and find a way of overcoming this threat.

Ways to overcome knowledge loss

To avoid various kinds of knowledge loss described above, organizations may take a range of diversified measures. An example of one such measure is knowledge retention. It is a relatively new sub-discipline of knowledge management and deals with cases where expert knowledge workers leave organizations after long periods of time (Levy, 2011). Retention of knowledge can be explained as maintaining (as opposed to losing) important knowledge that exists in the heads of people and is essential to the overall functioning of an organisation (Martins and Martins, 2011). This knowledge

does not necessarily have to be connected with products/services or other internal issues in the company.

For example, Parise et al. (2006) suggest performing an organizational network analysis in a knowledge-retention strategy, arguing that employees who leave companies take more than what they know; this means that they also take critical knowledge about who they know. De Long (2004) has suggested that effective knowledge retention actions require a holistic approach that integrates elements of HR infrastructure, culture, transfer practices reliant on the knowledge involved, and supporting IT applications. All in all, an appropriate knowledge-retention strategy can help in overcoming the problem of losing knowledge on important stakeholders, strategic partners or key customers.

As the amounts of tacit knowledge kept away in employees' heads are enormous, it is impossible to retain all the knowledge of staff members. Therefore, organizations should focus on retention of critical knowledge (Hislop, 2005; Durst et al., 2015). Knowledge retention projects, according to Levy (2011), should consist of steps where knowledge to be retained is exactly defined, together with determination of the method to retain it.

If knowledge is not retained, organizations can face problems with learning from past experiences and from the consequences of past actions, such as: reinventing the wheel, unlearned lessons or a pattern of repeated mistakes (Martins and Martins, 2011). That is why organizations are encouraged to focus on developing a formal retention strategy to retain critical and highly specialized knowledge (Juliano, 2004).

Protective mechanisms can also be applied by organizations to prevent knowledge leakage or knowledge spillover. Some knowledge can be secured by legal means (e.g. copyrights, patents, or trademarks). Companies may also be cautious in selecting outsourcing and cooperating partners to minimize the risk of improper knowledge usage by these parties. Another potential way of overcoming knowledge loss are safety-oriented knowledge management processes. These are processes designed to protect knowledge within an organization from illegal or inappropriate use or theft (Gold et al., 2001).

Despite the obvious financial and non-financial consequences of knowledge loss, organizations seem to underestimate the significance of knowledge retention and other means of protecting their knowledge. As Durst and Wilhelm (2011) report, organizations often notice the effects of knowledge loss only when a staff member has already left the company or is absent for a long time. Similar is the case with knowledge

DOI: 10.7206/jmba.ce.2450-7814.203

leakage or spillover – only when faced with it, organizations start coping with the consequences thereof.

Knowledge safety

Both knowledge loss and knowledge retention have been explained so far and considered mostly in the context of human resources – which is to mean employees that take away their knowledge and so, their knowledge needs to be somehow preserved by knowledge retention activities before their departure (e.g. Joe et al., 2013; Schmitt et al., 2012; Eckardt et al., 2014). However, knowledge can also be lost in a more technical context, i.e. if there is a database with clients, enriched with personal notes on each customer provided by an employee and this database is somehow lost (e.g. due to an equipment failure), it can be also treated as knowledge loss. Such knowledge loss was reported in a study by Durst et al. (2015), where a crash of an entire computer system resulted in a financial impact and a partial knowledge loss. In general, organizational knowledge can be lost in many ways: it can be stolen, it can be forgotten, damaged, or simply lost by losing an employee or knowledge stored in a certain form. Taking that into account, there appears an important question concerning knowledge safety – is knowledge in a given organization safe from all of the abovementioned risks? Therefore, knowledge safety can be defined in the following way:

> "The state of organizational knowledge not being endangered with or exposed to loss, leakage, attrition, oblivion, waste or theft, regardless of the potential sources of these phenomena. Knowledge safety can be ensured in two ways: 1. protecting knowledge from loss, leakage, attrition, oblivion, waste or theft by eliminating their potential sources; 2. retaining knowledge in the organizational setting and applying protection mechanisms to this knowledge".

Methodology

On the basis of literature review and the proposed definition of knowledge safety, three research questions have been formulated:

1. How do organizations understand knowledge safety?
2. What kind of potential hazards endangering organizational knowledge safety do they identify?
3. What kind of actions do they undertake on an everyday basis to ensure knowledge safety?

To answer these research questions, a case study approach has been applied. The rationale is as follows. Firstly, the issue of knowledge safety has not been explored so far and therefore, a study based on a qualitative method is appropriate to analyse it. Secondly, case study methodology allows for making observations and gathering information on new phenomena (Yin, 1989). Thirdly, the said case study approach is suitable given the descriptive and exploratory nature of the research and the potential complexity of the investigated issue (Leedy and Omrod, 2005).

The study involved semi-structured interviews with key informants who were expected to be knowledgeable about knowledge issues in their respective companies, i.e. either the owner or the general manager of a given enterprise. Companies were selected based on their convenient accessibility and proximity to the researcher (convenience sampling). This method is very useful in getting general ideas about the phenomenon of interest (Chong et al., 2011). Before each interview, the purpose of the study was presented to research subjects, followed by assurance of anonymity. Before the research commenced, all of the interviewees had to sign an agreement to participate in the study and to be recorded. Names of the companies and interviewees have been anonymized for confidentiality reasons. The interviews lasted thirty minutes on average and were conducted at the company premises. Afterwards, the interview data was recorded and subsequently transcribed with care (Meyer, 2001). In addition, for the purpose of triangulation, the transcribed interviews were analysed along with observational field notes and information published on the companies' websites (Suter, 2012). The observational field notes concerned the atmosphere of trust, the mood of the recipients, as well as their behaviour, reactions to the questions, and willingness to answer the questions, etc. The companies' websites were examined with regard to descriptions of services they offered, their history, market presence, and other materials made available.

10 case studies were covered in total. These were small and medium-sized companies located in the province of Pomerania in Poland. Multi-case sampling was chosen to add confidence to the findings (Meyer, 2001). Although the number of cases was limited because of accessibility, resources, and time constraints, a similar number of cases had been presented in other qualitative research on SMEs and their knowledge (e.g. McAdam and Keogh, 2004; Bishop et al., 2008; Nunes et al., 2006; Ndlela and du Toit, 2001).

The companies selected for the performed analysis had to belong to the SME knowledge-intensive service sector and be located in the Pomeranian region. Knowledge-intensive companies were chosen as the object of study because knowledge plays a crucial role in their functioning (Mangiarotti, 2012). Therefore, they should be concerned with

 DOI: 10.7206/jmba.ce.2450-7814.203

knowledge safety and they can be expected to be taking some measures to guarantee it. The firms subject to analysis varied with regard to the number of employees and the area of operation (details in Table 1). The interviews and the analysis of the observational field notes and of the information published on the companies' websites were conducted at the end of 2013 and the beginning of 2014.

Table 1. Characteristics of the case companies

Company	Main activity	Number of employees
Company A	Financial services	10–15
Company B	Advisory and consultancy	10–15
Company C	Design of websites and promotion materials	Less than 10
Company D	Design of telecommunication systems	10
Company E	Design of electronic devices	Less than 10
Company F	SaaS (Software as a Service) provider	Less than 10
Company G	Telecommunication services	80
Company H	Construction and supervisory services	6
Company I	Multimedia applications and Business Intelligence	7
Company J	Educational and training services	15

Source: own study.

The author has taken advantage of inductive approach to analyse the collected data as this method is suitable for performing analyses with little or no predetermined theory or framework, when little or nothing is known about the examined phenomenon (Burnard et al., 2008). To be more precise, the thematic content analysis method (Krippendorff, 2004; Fereday and Muir-Cochrane, 2006) has been applied where analysis themes and subthemes have been defined and then matched with the recorded and transcribed statements.

Presentation of findings

This section covers the findings of the conducted study. For the sake of clarification of the details about the featured companies, the notation from Table 1 will be applied.

The first question concerned the understanding of knowledge safety. It appears that the examined companies understand this notion in different ways. Some companies understand it with regard to their technical solutions and databases only. For example, Company E concentrates on the safety of their base of experience – a database containing past experience, projects, costs, failures, etc. Similarly, Company G perceives it as the safety of all of their technical tools that they use, while Company C sees it as the safety of their IT systems.

Other companies view knowledge safety in the context of their employees possessing this knowledge. For example, the owner of Company B stated that *the problem of knowledge safety is connected with human resources. You can protect yourself against technologies, but not against humans. If somebody wants to steal knowledge from us, they will do it.* Also, the owner of Company A concluded that the value of the company resided in the company's employees and their knowledge, and this knowledge could not be protected. In other words, if an employee wants to leave and take such knowledge with them, they will do it.

There are also companies that understand and view knowledge safety in both dimensions: in the technical one and in the human one. For example, Company J distinguishes safety of their technical solutions (Google Drive, where they place all of their files) and safety of the knowledge possessed by their employees. They perceive knowledge safety through the aspect of protecting it from theft (technical solutions) or loss (employee leaving the company/being "stolen" by the competition). Also, Company H understands knowledge safety as the safety of their information uploaded to a server and the protection against industrial espionage.

The second question was about the perception of the potential hazards endangering the knowledge safety of the interviewed firms. Interestingly enough, although the companies participating in the research are aware of some risks connected with knowledge safety, in most cases they are not concerned too much about these risks. For example, Company J sees the body of knowledge uploaded to Google Drive as safe. As the owner of this company said, *We trust these solutions. In my opinion, the data stored in the cloud is more secure than the data stored on drives, because like all systems, passwords that are on the computers of employees are usually a joke so it is better to keep the knowledge somewhere on a really protected server.* Company J is also not afraid of somebody stealing their knowledge: *We are not afraid of competitions, as it would be difficult for the competitors to take an employee from us and start the process with this knowledge because this knowledge is spread around.* Moreover, Company F does not see losing an employee as a potential problem. Their competitive situation is so favourable

DOI: 10.7206/jmba.ce.2450-7814.203

that even if new competitors entered the market, it would be beneficial for them because they would help them educate potential customers.

Company G claims that they have had a certain level of safety ensured since the beginning of their activity. As time went by, this level was raised for all their tools and today, they perceive this level as appropriate. They do not think about further changes of the current safety level.

Company H is aware of the fact that knowledge is kept mainly in the heads of its employees and only a part of it is stored in a database. However, they are not afraid of losing an employee with this knowledge because many employees exchange their tasks. A loss of an employee involves a brief moment of disturbance, but is not perceived as a big problem.

Company I considers its knowledge as safe, although its owner is aware of the potential risks. The first of these risks is related to the software they produce and the second one – with the staff that may leave the company to work for a larger business. They are not very concerned with the issue of knowledge safety because – in their opinion – not much can be done to improve it.

The third question concerned measures taken by the interviewed companies to ensure knowledge safety on an everyday basis. The variety of these measures is quite large and dependent on the type of knowledge risks the companies perceive as threatening their knowledge safety. For example, Company E is concerned with its database of experience and therefore, performs regular back-ups and stores its e-mails for many years.

Company B provides its employees with only the knowledge that they need to perform their tasks. *We share different knowledge with different people. If we know that this most precious knowledge is only in the heads of some employees and it cannot be taken away easily (is not in the written form), then it is safe*. The company also makes sure to motivate its employees to encourage them to share their knowledge internally, not externally.

Company I has two ways of dealing with knowledge safety. The first one is about making appropriate agreements with its customers and employees, and the second one is about hiring young interns, who are less likely to leave the company than its experienced professionals.

Furthermore, Company J undertakes some action to ensure the safety of the knowledge possessed by its employees. The company understands the risk of their staff leaving

the firm as they hire mostly young, creative people who might start searching for new paths of development. *We take advantage of rotation of positions and training of other employees to store and transfer the knowledge inside the organization. We also have a mentoring system, so that our employees can exchange their knowledge mutually. These actions are supposed to prevent knowledge loss and ensure knowledge safety.*

DOI: 10.7206/jmba.ce.2450-7814.203

Some companies deal with provision of knowledge safety in a peculiar way. For example, the owner of Company A, in order to avoid the loss of employees and their knowledge, avoids investing in training for the company's employees. The person has some bad experience with employees being well-trained and leaving the company for another one or to set up their own business.

However, some of the companies claim that they do not take any measures on an everyday basis to ensure knowledge safety. For example, Company J stated that *Our technology is very cheap and we want to sell it widely, so its theft is not a big threat to us. That is why we do not concentrate on this treat, because these are costs to ensure the safety of our knowledge*. Company D does not aim to protect its knowledge as there is no such need. *In our branch two years is like a century. After two years everything becomes obsolete. In the past, we used to race for patents, but now, it does not pay off. It does not make sense*. Also, Company G does not see the point of dealing with knowledge safety on an everyday basis. *We do not need to deal with knowledge safety because it is a standard thing for our operations. We have some critical systems, which can be accessed only from certain locations and there are non-critical systems, which can be accessed from many different locations. They are protected with passwords. We do not deal with knowledge safety because it is handled in a systemic way.*

Some firms are not concerned with their knowledge safety because they do not think their knowledge is potentially of much use to others. For example, Company H stated: *We do not have such crucial knowledge, I do not imagine someone needing this knowledge apart from us*. That is why they do not undertake any actions to ensure knowledge safety.

Discussion and conclusions

This paper examines the concept of knowledge safety in service companies operating in the knowledge-intensive SME sector. Keeping in mind that knowledge safety is a new concept, the study contributes to a better understanding of knowledge protection issues in small and medium-sized companies and lays grounds for further research. It contributes to earlier studies devoted to knowledge loss (e.g. Martins and Martins

2011; Durst and Wilhelm 2011), knowledge leakage (Ahmad et al., 2014), knowledge spillover (Durst and Zieba, 2017), knowledge forgetting (De Holan and Phillips 2004; Cegarra-Navarro, 2012), unlearning (Rebernik and Širec, 2007) and waste (Ferenhof et al., 2015), and knowledge retention (e.g. Levy, 2011; Parise et al., 2006) as it integrates the aspect of losing knowledge in various ways (e.g. due to human or technological factors) with measures to be taken to prevent it (e.g. knowledge retention).

The findings of the study show that knowledge safety is perceived by the examined companies from two perspectives:

- **technical perspective** – connected with the safety of technical solutions, tools, databases possessed by companies;
- **human perspective** – connected with human issues, e.g. potential loss of employees leaving for other companies/competitors and taking their knowledge with them.

Some companies view knowledge safety mostly in a technical sense, some see it in a human context, while others understand it as a combination of the two. There is no single, uniform view of knowledge safety among the firms included in the study. It can result from the fact that different kinds of knowledge can be protected in various ways and therefore, it would be improper to limit the approach towards knowledge safety to one predominant view only.

Most of the interviewed companies do not consider knowledge safety as a problematic issue. They are well-aware of the potential hazards connected with the knowledge they possess, but in many cases, they do not undertake any everyday actions to prevent their occurrence. There are several reasons for that. First of all, some risks are not, in their opinion, likely to occur, e.g. industrial espionage. Second, some companies do not consider their knowledge as potentially valuable to other companies or competitors. Third, the costs of ensuring knowledge safety and, for example, preventing knowledge loss would be too high or exceeding the costs of losing knowledge. Fourth, some problems with knowledge safety are perceived as natural and "something to live with" instead of "to be prevented from happening". Fifth, SMEs suffer from limited financial resources and therefore are reluctant to invest in preventive measures. Sixth, small organizations prefer operating in an informal and flexible manner (Panagiotakopoulos, 2012) and as such, do not concentrate often on formal analyses and solutions. Finally, such companies tend to have no time to think about the future or anticipate potential risks, so they also do not deal with such risks as far as the knowledge in their possession is concerned.

Companies that do intend to take measures to protect their knowledge can do it in several different ways, such as:

- by motivating employees to share knowledge and not to take it away;
- by reducing the potential "attractiveness" of their employees on the labour market (e.g. by limiting the possibilities of training);
- by transferring and storing crucial knowledge in an transparent form in databases;
- by sharing crucial knowledge only with a limited number of people in the organization;
- by doing back-ups of their data and databases;
- by choosing solutions/tools that are sufficiently protected;
- by providing different levels of access to bodies of knowledge – only to those who need such knowledge to perform their tasks.

The abovementioned ways have been utilized by different companies, but are not applied by all of them.

Implications and further research directions

The study provides company managers and owners with some suggestions on the issues of knowledge safety. It can serve as an indication of what aspects managers should consider when analysing their knowledge safety. From the point of view of research, the findings contribute to a better understanding of the concept of knowledge safety in the context of the SME environment. This topic is quite significant as the lack of knowledge safety could potentially have detrimental effects on a small or medium-sized company.

The presented study has several limitations, though. The first one results from the fact that the data covered has been collected in 10 SMEs operating in the Pomeranian region of Poland; therefore, the reliability and universality of the findings is limited. Second, only one person from each company has been interviewed, which may limit the objectivity of the research results. Third, the companies examined are mostly small or even micro businesses, which reduces the applicability of the research results to medium-sized businesses. Finally, the research is of a preliminary character and a further in-depth exploration is required.

DOI: 10.7206/jmba.ce.2450-7814.203

There are further research possibilities in the area of knowledge safety proposed. The first issue that could be investigated concerns the matter of which aspect of knowledge safety is the most crucial from the point of view of particular types of SMEs. For example, some might feel more exposed to knowledge theft, while others – with knowledge spillover. The second one could involve examination of potential benefits of ensuring knowledge safety versus the cost of losing knowledge. Finally, a quantitative study on knowledge safety could offer further insights into the state of the art in the whole SME sector.

Acknowledgements

This study has been conducted within the research project entitled "Knowledge management in small and medium-sized enterprises (SMEs) offering knowledge intensive business services", and funded by the Polish National Science Centre on the basis of Decision No. DEC/2011/01/D/HS4/04111.

The draft version of this paper was presented during the 17th European Conference on Knowledge Management in Belfast, UK.

References

Ahmad, A., Bosua, R. and Scheepers, R. (2014). Protecting organizational competitive advantage: A knowledge leakage perspective. *Computers and Safety*, *42*: 27–39, https://doi.org/10.1016/j.cose.2014.01.001

Awad, E.M. and Ghaziri, H.M. (2004). *Knowledge Management*. Pearson Education.

Bishop, J., Bouchlaghem, D., Glass, J. and Matsumoto, I. (2008). Ensuring the effectiveness of a knowledge management initiative. *Journal of Knowledge Management*, *12*(4): 16–29, https://doi.org/10.1108/13673270810884228

Burnard, P., Gil, P., Stewart, K., Treasure, E. and Chadwick, B. (2008). Analysing and presenting qualitative data. *British Dental Journal*, *204*(8): 429–432, https://doi.org/10.1038/sj.bdj.2008.292

Cegarra-Navarro, J.G., Sánchez-Vidal, M.E. and Cegarra-Leiva, D. (2011). Balancing exploration and exploitation of knowledge through an unlearning context: An empirical investigation in SMEs. *Management Decision*, *49*(7): 1099–1119, https://doi.org/10.1108/00251741111151163

Cegarra-Navarro, J., Martinez-Martinez, A., Ortega Gutiérrez, J. and Luis Leal Rodríguez, A. (2013). Environmental knowledge, unlearning, and performance in hospitality companies. *Management Decision*, *51*(2): 341–360, https://doi.org/10.1108/00251741311301858

Chong, C.W., Chong, S.C. and Gan, G.C. (2011). Inter-organizational knowledge transfer needs among small and medium enterprises. *Library Review*, *60*(1): 37–52, https://doi.org/10.1108/00242531111100568

Dąbrowska, M. (2005). Knowledge and knowledge management in contemporary organizations: theoretical considerations. *Foundations of Control and Management Sciences*, *3*: 79–94.

de Holan, P.M. and Phillips, N. (2004). Remembrance of things past? The dynamics of organizational forgetting. *Management Science*, *50*(11): 1603–1613, https://doi.org/10.1287/mnsc.1040.0273

De Long, D.W. (2004). *Lost Knowledge: Confronting the Threat of an Aging Workforce*. Oxford: Oxford University Press, https://doi.org/10.1093/acprof:oso/9780195170979.001.0001

De Long, D.W. and Davenport, T. (2003). Better practices for retaining organizational knowledge: Lessons from the leading edge. *Employment Relations Today*, *30*(3): 51–63, https://doi.org/10.1002/ert.10098

Durst, S., Edvardsson, I.R. and Bruns, G. (2015). Knowledge Retention in SMEs – Insights into the building and construction industry. In: G.S. and V.A.J.C. Spender (eds.), *Culture, Innovation and Entrepreneurship: connecting the knowledge dots*. Matera: Institute of Knowledge Asset Management (IKAM).

Durst, S. and Wilhelm, S. (2011). Knowledge management in practice: insights into a medium-sized enterprise's exposure to knowledge loss. *Prometheus*, *29*(1): 23–38, https://doi.org/10.1080/08109028.2011.565693

Durst, S. and Zieba, M. (2017). Knowledge Risks – Towards a Taxonomy. *International Journal of Business Environment* (forthcoming), https://doi.org/10.1504/IJBE.2017.084705

Eckardt, R., Skaggs, B.C. and Youndt, M. (2014). Turnover and knowledge loss: An examination of the differential impact of production manager and worker turnover in service and manufacturing firms. *Journal of Management Studies*, *51*(7): 1025–1057, https://doi.org/10.1111/joms.12096

Edvardsson, I.R. (2006). Knowledge management in SMEs: the case of Icelandic firms. *Knowledge Management Research & Practice*, *4*(4): 275–282, https://doi.org/10.1057/palgrave.kmrp.8500111

Edvardsson, I.R. (2009). Is knowledge management losing ground? Development among Icelandic SMEs. *Knowledge Management Research and Practice*, *7*(1): 91–99, https://doi.org/10.1057/kmrp.2008.30

Fereday, J. and Muir-Cochrane, E. (2006). Demonstrating rigor using thematic analysis: a hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods*, *5*(1): 80–92, https://doi.org/10.1177/160940690600500107

Ferenhof, H., Durst, S. and 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

Gharajedaghi, J. (2007). Systems thinking: a case for second-order-learning. *The Learning Organization*, *14*(6): 473–479, https://doi.org/10.1108/09696470710825088

Gold, H.A., Malhotra, A., and Albert, S. (2001). Knowledge Management: An Organizational Capabilities Perspective. *Journal of Management Information Systems*, *18*(1): 185–214, https://doi.org/10.1080/07421222.2001.11045669

Hislop, D. (2005). *Knowledge Management in Organizations*. Oxford: Oxford University Press.

Holsapple, C.W. (2003). Knowledge and Its Attributes. In: *Handbook on Knowledge Management*. Berlin: Springer-Verlag, https://doi.org/10.1007/978-3-540-24748-7

Hutchinson, V. and Quintas, P. (2008). Do SMEs do knowledge management? Or simply manage what they know? *International Small Business Journal*, *26*(2): 131–134, https://doi.org/10.1177/0266242607086571

Joe, C., Yoong, P. and Patel, K. (2013). Knowledge loss when older experts leave knowledge-intensive organisations. *Journal of Knowledge Management*, *17*(6): 913–927, https://doi.org/10.1108/JKM-04-2013-0137

Juliano, J.J. (2004). Gen-X and Gen-Y: teaching them the business. *Public Utilities Fortnightly*, *142*(6): 82–85.

Krippendorff, K. (2004). *Content Analysis: An Introduction to its Methodology*. Thousand Oaks, CA: Sage.

DOI: 10.7206/jmba.ce.2450-7814.203

Leedy, P.D. and Omrod, J.P. (2005). *Practical Research – Planning and Design*. Upper Saddle, NJ: Pearson.

Levy, M. (2011). Knowledge retention: minimizing organizational business loss. *Journal of Knowledge Management*, *15*(4): 582–600, https://doi.org/10.1108/13673271111151974

Liebeskind, J.P. (1996). Knowledge, strategy, and the theory of the firm. *Strategic Management Journa*l, *17*(S2): 93–107, https://doi.org/10.1002/smj.4250171109

Mangiarotti, G. (2012). Knowledge management practices and innovation propensity: a firm level analysis from Luxembourg. *International Journal of Technology Management*, *58*(3/4): 261–283, https://doi.org/10.1504/IJTM.2012.046618

Markóczy, L. (1994). Modes of Organizational Learning. Institutional Change and Hungarian Joint Ventures. *International Studies of Management & Organization*, *24*(4): 5–30, https://doi.org/10.1080/00208825.1994.11656642

Martins, E. and 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, https://doi.org/10.1177/1350507608096040

McAdam, R. and Keogh, W. (2004). Transitioning towards creativity and innovation measurement in SMEs. *Creativity and Innovation Management*, *13*(2): 126–139, https://doi.org/10.1111/j.0963-1690.2004.00300.x

Meyer, C.B. (2001). A Case in Case Study Methodology. *Field Methods*, *13*(4): 329–352, https://doi.org/10.1177/1525822X0101300402

Mohamed, S., Mynors, D., Andrew, G., Chan, P., Coles, R. and Walsh, K. (2007). Unearthing key drivers of knowledge leakage. *International Journal of Knowledge Management Studies*, *1*(3–4): 456–470, https://doi.org/10.1504/IJKMS.2007.012535

Ndlela, L.T. and du Toit, A.S.A. (2001). Establishing a knowledge management program for competitive advantage in an enterprise. *International Journal of Information Management*, *21*(2): 151–165, https://doi.org/10.1016/S0268-4012(01)00007-X

Nunes, M.B., Annansingh, F., Eaglestone, B. and Wakefield, R. (2006). Knowledge management issues in knowledge-intensive SMEs. *Journal of Documentation*, *62*(1): 101–119, https://doi.org/10.1108/00220410610642075

Pablos, P.O. de (2002). Evidence of intellectual capital measurement from Asia, Europe and the Middle East. *Journal of Intellectual Capital*, *3*(3): 287–302, https://doi.org/10.1108/14691930210435624

Panagiotakopoulos, A. (2012). Staff "poaching" in the small business context: overcoming this key barrier to training. *Industrial and Commercial Training*, *44*(6): 326–333, https://doi.org/10.1108/00197851211254752

Parise, S., Cross, R. and Davenport, T.H. (2006). Strategies for preventing a knowledge-loss crisis. *MIT Sloan Management Review*, *47*(4): 31–38.

Rebernik, M. and Širec, K. (2007). Fostering innovation by unlearning tacit knowledge. *Kybernetes*, *36*(3/4): 406–419, https://doi.org/10.1108/03684920710747039

Schmitt, A., Borzillo, S. and Probst, G. (2012). Don't let knowledge walk away: Knowledge retention during employee downsizing. *Management Learning*, *43*(1): 53–74, https://doi.org/10.1177/1350507611411630