Why should we investigate knowledge risks incidents?

Why should we investigate knowledge risks incidents? - Lessons from four cases.

Stefan Thalmann
Center for Business Analytics and Data Science
University of Graz,
Graz, Austria
stefan.thalmann@uni-graz.at

Ilona Ilvonen
Unit of Information and Knowledge Management
Tampere University
Tampere, Finland
Ilona.ilvonen@tuni.fi

Abstract

In a knowledge-based economy, knowledge has become the most important source for competitive advantage. Thus, organizations spend more attention on the protection of knowledge and also research on knowledge protection has gained increasing attention in the past years. However, knowledge protection research mainly focuses on the design of preventive measures and little is published about real incidents or reactive measures. Learning from failure and from incidents is important to improve current practice. This paper reflects on four cases of real knowledge risk incidents. We discuss ways to prevent or delay knowledge spillovers and the importance of knowing the threats in order to prevent them. In addition to preventive measures, we highlight that companies need to have reactive measures in place. Finally, based on our insights we discuss why analyzing incidents in addition to identified threats is important for practice as well as academia.

1. Introduction

Researchers widely acknowledge that knowledge is strategically the most significant resource and therefore needs to be protected [22] from loss, obsolescence, unauthorized exposure, unauthorized modification, and erroneous assimilation [14] Scholars argue, that firms' competitive advantages depend on their ability to protect their critical knowledge [24]. Hence, the importance of knowledge protection is widely emphasized and its strategic nature is exposed [26].

Despite general remarks why knowledge protection is important, not much is published about real consequences of the realization of knowledge risks. For the risk of losing knowledge inside the company, e.g., due to employee retirement, studies try to quantify the impact of knowledge loss and suggest that knowledge loss causes organizational problems like low productivity or reduced moral [31], others investigate the relationship between knowledge loss and performance [25] or the skills of responsible staff [19]. Also for risk of losing reputation some studies can be found [e.g. 36, 42]. Of the risk of unwanted knowledge spillovers and thus the risk of losing the exclusiveness of knowledge very little is known of the actual consequences of risk incidents. Scholars describe the impact in general terms, like "competitors use this knowledge to gain competitive advantage" [9] or assume that the impact is obvious, like "consequences are easy to imagine" [10] and thus does not need to be described further. Although it may be easy to imagine different consequences, learning from incidents requires describing and analyzing the consequences in detail.

Reporting about concrete failures is frequently avoided as this is connotated with a blaming and hence it is difficult to investigate concrete incidents. This is particularly true for knowledge risks as they have a strong link to the competitiveness of the company due to the strategic and competitive importance of knowledge. Research shows that managers assume reporting about such incidents will have negative effects on investors and the firm's reputation [35].

Despite the challenges, it seems that investigating real knowledge risk incidents provide an important research opportunity on the one hand and has a high relevance for practice on the other hand. In general, systematic research on failure provides valuable insights for research as well as for practice [13]. This leads to the research question of this paper:

RQ: What are concrete knowledge risk incidents and what can we learn from such incidents?

To answer the research question, the authors first review the existing literature on knowledge protection with a focus on knowledge risk incidents. Based on this review the authors conduct a secondary data analysis of interview material collected in three studies

URI: https://hdl.handle.net/10125/64349
978-0-9981331-3-3

focusing on knowledge protection. After presenting four cases in which a knowledge risk materializes, lessons learned for research as well as for practice are discussed.

2. Related work

Knowledge protection is defined as the collection of the formal practices that organizations enforce and the informal practices that individuals perform to prevent unwanted disclosure, spillover, or loss of knowledge [38].

From this definition we can derive that knowledge risks (that the protection is done to prevent) are linked to incidents, where knowledge is disclosed, leaked or lost. According to Durst & Zieba [10] 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. This leads us to define a knowledge risk incident as an knowledge-related event that disrupts the functioning of an organization or its competitive position.

There is a number of articles that concentrate on reviewing the past research on knowledge protection and knowledge risks [e.g. 10, 16, 27]. These reviews more or less agree that there is much to do especially in terms of empirical work in this area. Understanding knowledge risks and the consequences of them ultimately requires understanding real world incidents, but empirical work on the topic is scarce; a lot of the work so far has been conceptual or theoretical in nature [8].

In addition to focusing on the definitions of knowledge risks, the conceptual approaches to knowledge risk management or knowledge protection range from management frameworks [e.g. 18, 32, 40] and conceptual models [e.g. 12, 26]; collections of measures [39] to taxonomies [10, 41]. Most conceptual works propose frameworks supporting the understanding of the complex phenomenon called knowledge risk audits better management in organizations. A lot of the focus in the management frameworks is on understanding, preventing or avoiding knowledge risk incidents [17, 30].

The perspective of continuity planning that is present in the information security management literature [e.g. 6, 34] is not so much regarded in knowledge risk literature. A focus on continuity planning would encourage preparing for what to do in case of an incident happens [34]. However, the knowledge risk frameworks that draw on the information security neglect this aspect so far. The cyclical nature of the management processes can be interpreted to aim for learning from incidents and preparing for them in the future, but the actual continuity planning efforts are scarcely addressed in literature [e.g. 15, 32]. Continuity planning in the knowledge risk domain is instead brought up mainly in the context of employee turnover [4, 20, 33]

Most of the empirical studies that concern knowledge risks aim to understand the perceptions on knowledge risks or on existing management practices of organizations. The range of methods used to achieve this general goal is broad [8]. The expectation in the empirical work is to discover how organizations protect their knowledge, and what they have done to proactively mitigate knowledge risks.

The perspective of learning from failures [11] is not much present in the papers, although incidents may be discussed as a motivation for the papers [e.g. 1]. This does not necessarily mean that the organizations do not strive to learn from failures. However, it either indicates lack of willingness to discuss this with researchers, or lack of interest for failure from researchers, or both. For example, a google scholar search for “knowledge risk incident” or “knowledge loss incident” or “knowledge risk failure” at the time of writing this paper provides no results. Although a systematic review with a wide range of search terms would be needed to locate all possible discussions of knowledge risk incidents that may have been published, at present it seems, that they are not much willingly discussed in the open, even as anonymous case studies.

The most interesting part of the definition of knowledge risk we use in this paper, is the “severity of adverse effects”, or in other terms, the consequences of knowledge risk incidents. For example, Ilvonen et al. [16] present a classification of knowledge risks and protection management mechanisms, but don’t really touch on the consequences of knowledge risk incidents. Massingham [30] goes more to the direction of assessing the consequences, but also this approach leaves the consequences vague. An integral part of management, however, is the decision making of how much money is spent on different activities, and why.

Thalmann et al. [40] propose a risk management framework inspired from IT-risk management: how to design and implement countermeasures and how to check if all measures are in place. In this and other similar research it is assumed that the measures are effective in preventing knowledge risk realization. One aspect of knowledge risks defined above is knowledge loss. Knowledge loss due to leaving employees is one of the more studied areas connected to knowledge risks [e.g. 18, 23, 31]. Even in this domain studying the impact of knowledge risk incidents empirically is scarce [e.g. 31] and the perspective of response is lacking.

Research on real incidents is important to better understand the nature of knowledge risk itself and to investigate the effectiveness of organizational risk management frameworks. The authors acknowledge that investigating real incidents is challenging as this is a sensitive topic, however it is important for further developing the research on knowledge risks. As knowledge risk management is heavily inspired by information security management [19], we should also follow the research tradition of information security management and rigorously investigate and learn from incidents.

3. Method

This paper presents a secondary analysis [37] of three studies focusing on knowledge risks and knowledge protection conducted between 2012 and 2018. Although secondary analysis as a research method is more widely used in the health care sector [37], especially because it is suitable for studying sensitive issues, it is sometimes used also in Information Systems research e.g. [2, 5].

As the perspective of learning from knowledge risk incidents rose as an interesting perspective to us, we went back to our previous interview materials, and further analyzed the scarce mentions of knowledge risk incidents present in our interview transcripts.

We had asked about knowledge risk realization in all our three interview studies, but only very few interviewees answered directly. Most of the interviewees avoided the issue and answered on abstract levels and we focused the interview discussion on other knowledge risk aspects as risk incidents were not the focus of the study at the time. The interviewees who talked about the incidents were also concerned about linking an incident directly with their company. Hence, after re-coding of the transcripts we realized that risk realization is a highly sensitive topic.

Overall, we re-analyzed three studies with a total of 129 interviewees (see table 1 for details). All interviews were recorded and transcribed and had a focus on knowledge protection and knowledge risks and were analyzed, i.e. coded previously by one of the authors. For the purpose of this paper, we recoded the interviews focusing on knowledge risk realization and incidents. Due to different interview languages, i.e. English, Finnish and German every author coded the interviews he or she conducted, and we had various synchronization meetings about the emerged code set´s. Finally, we identified four cases where an actual incident and the consequences were discussed by the interviewees.

Table 1. Interview material

ID	No of Interviewees	duration	Countries	Year conducted
#1	7	avg 55 minutes	FI	2012
#2	91	avg 62 minutes	AT, DE, UK	2013 and 2014
#3	31	avg 40 minutes	AT, CH, DE, IT, PT	2017 and 2018

Our experience as researchers is that knowledge protection is a topic that organizations treat with caution and are not willing to disclose detailed information about concrete incidents and in particular about their impact. In fact, in some cases the condition for agreeing to the interview has been that details of what has happened in the organization are not discussed. Despite the shortcomings of the data, the cases that are presented in this paper warrant attention.

4. Four cases of incidents

Based on our analysis we present four cases: case 4.1 has is origin in study #3, case 4.2 and 4.3 in study #2 and case 4.4. in study #1.

4.1 Violation of trust

The first case considers the trust between organizations, and the consequent risk that this trust is violated. In this case a small tool manufacturer shared details of a product (construction plans) and also production details with a large enterprise that was also one of its main customers. The tool manufacturer shared many details of its products with the large enterprise, because of a long and successful business relationship and due to the high importance (revenue share) of this big customer. But the interviewee described what happens if you do not spend enough efforts into protection:

> *"No no it's worthwhile to take any action to protect. It's worthwhile. For example, one of our <name of tool> was copied in China. But unfortunately, this was due to some un-loyal customer. So, you cannot … when talking about trust it's that …a customer asked [this company in China] to copy one of our tools to buy it cheaper. So when you have this kind of customers … you are completely defeated. So, you cannot do anything. You can only react. […] But … also after this fact that happened, so we are very sensitive to any kind of information we give outside. Very sensitive."*

The interviewee also concluded that collaboration with trust and without protection might be the best basis for a fruitful knowledge-based collaboration, but a company should never solely rely on trust as they then have no other measures to react.

> *"If I trust the other party and I don't expect surprises, so very honest very clear and so on, I believe that for me it is the best way of getting the maximum output of the collaboration. […] but not just be to open, you know […] I am not talking about the Open Kimono approach, okay? I don't know if you understand what I'm talking about when I say Open Kimono. Japanese they say Open Kimono it means that usually Japanese they are naked under the Kimono. So when they open the Kimono they show them completely naked."*

Within the interview it became clear that the incident with the un-loyal customer really shaped the mind of the interviewee and consequently the mindset of the company. The situation of not having the control over the process and the perception that "you can only react", really made him and his company more careful. Additionally, to the financial losses, this insecurity around the case required massive management attention and caused a massive cognitive load to all involved people. Hence, he and his company are very keen of maintaining control and not to be "naked under the kimono" anymore.

4.2 Spillover

In our second case, concerning knowledge spillover, the owner of a small electrical engineering company reported about an innovation he made to control the bacteria within a pig breeding ventilation system. The control mechanism ensured that the bacteria in the air ventilation reduced the smell of the pigs significantly, which enhanced the acceptance of pig breeding in the area. The electrical engineer was fully aware that this control mechanism was an important competitive advantage in the market, and he acquired lots of lucrative contracts based on this technology.

> *"The control mechanism for the chemicals and the bacteria was key and we protected the knowledge in such a way that nobody can get it. This is crucial, because apart from the control the rest of the installation is trivial and anybody can do this. But the contract is coupled, and we did this four years more or less exclusively in northern Germany."*

To secure this knowledge, he actively protected this knowledge by applying technical measures such as encryption, he instructed his employees and talked very carefully about this innovation. Additionally, the company also applied measures to make reverse engineering more challenging as well as measures to confuse his competitors. He was very aware of the threat and of the main competitors:

> *"Dominantly we used technical measures, like encryption but we also added additional things to the control unit to make reverse engineering more challenging. Secrecy was strictly enforced, and we also tried to confuse our competitors by spreading fake information. But if you have a competitive advantage in the market, your competitors will try everything to get it and what you can do is to gain time by such measures."*

He was successful with his knowledge protection strategy, but after four years the competitors were able to reverse engineer the control mechanism. The contract volume of 500.000€ per year (which is substantial for an SME with 20 employees) has since diminished

> *"We defended this exclusive knowledge "tooth and nail" for four years, which secured us ½ million € revenue each year. But now the knowledge is out, and we don't get the contracts anymore. Because other companies are cheaper or more close to the customer."*

This shows clearly that knowledge protection pays off and that knowledge spillover can result in concrete financial losses. We also asked the owner of this construction company about patenting:

> *"Patenting is something for large enterprises having lots of money and tough lawyers. If I patent this control mechanism it is away, as I have to make this mechanism publicly available. Others could adapt this easily and I do not have the money to fight a lawsuit and the success is also questionable."*

Hence, the interviewee clearly described the limitation of formal legal protection measures for process knowledge and especially the challenge of enforcing legal measures as a small company.

4.3 Immature Idea

The third case considers the complex risks related to immature ideas. In this case an innovation manager from a small company operating in the field of medical engineering reported about an incident. He had an idea how to construct an implant in a more robust way, but he needed process knowledge how to create suitable molds for the product. Thus, he joined a network meeting of his local network dealing with life science topics. Many different companies from the region interested in the topic participated and he talked with several experts from the material sciences.

"Talking with people from other domains is usually most interesting, you get fresh ideas and for some innovative projects you just need other partners, especially as a small company."

Intentionally (to protect the idea), he never explained his new idea in detail, but asked questions. His strategy was to discuss on a high level with the other companies in order to identify the right partner for implementation. He was convinced that without specific knowledge about the application domain of the implant the idea was protected.

"If you talk with your competitors from your domain, they have more or less the same mindset and background knowledge. We will understand soon. If you discuss your idea with people from other fields, sure - you have to be careful, but it's unlikely that they will understand and even if they understand the idea, it's unlikely that they will exploit your idea."

However, there was also a competitor in the room who had a trusted relationship with one of the material sciences companies. This person talked with his friend and they discovered the idea of the innovation manager.

"However, never say never! In this case I talked with a material science guy and he was extremely interested and very competent. He had lots of good ideas and comments and talked more and more. It is a giving and taking and you get trust over time, and of course I wanted to find a collaboration partner for implementing my idea. But he had already a working relationship with one of my competitors and yes the idea was away!"

The interviewee explained that he balanced knowledge sharing and protection in a sense that if he perceived a good return, he would also disclose more knowledge. This on the one hand because he wants to push the discussion, and on the other hand because he wanted to build trust during the conversation. However, the wiggle room is not so big for ideas as he explained:

"You know an idea has not so many details you can hide - it is like a raw egg with a soft skin. You have to find the solution way - the shell, it is the novelty and exclusiveness which counts for an idea."

As he reflects, an idea is very sensitive and like a raw egg. The complexity is very low, in this context you cannot hide many details and hence it is relatively easy for a knowledgeable expert to grasp the core idea. The other person together with the material science company finally pushed the idea to a product and the innovation manager was not able to monetize his idea.

"They did it! I did not manage to find a suitable partner in time and finally they exploited the idea first."

Because of the market structure and the size of the company he did not follow-up on this idea and it was a lost opportunity for the company.

4.4 Turnover

The last case we discuss is turnover of employees. Employee turnover can have multiple reasons, and this was a theme that was widely discussed in some of the interviews. However, the discussion of actual incidents caused by turnover in more detail was not so common. In this section we bring out two incident situations: retirement of a long-term manager, and an unexpected death of an employee.

"there is always a threat that knowledge will leave the company. ... We don't have a solid chain of supervisors who would think about knowledge [and its continuance]. We have a project organization, and the project manager does not necessarily think about the knowledge from the development point of view as much as from the user point of view"

As this interview quote from a middle-sized company highlights, the risks linked to knowledge turnover need to be identified. If the managers are not interested in the long-term development of the organization, they do not necessarily focus on the importance of individual employees to the long-term survival of the organization. The situation is particular challenging when the person leaving is the person who should do the identification: when the manager leaves. This happened in the interviewed company.

"There is actually only one person who knows all our customers and how to do business with them, and the customer entity. And now when this person is going to retire, we have established this sort of master-apprentice setting to approach this problem. The apprentice will follow along for almost a year. And this is done solely because of the knowledge. On account of the person who is retiring, I don't think there is a single document about what he has been doing for the past [few] years"

In the company the retiring senior manager had clearly managed to recruit the right people and despite shortcomings in his own documentation process, instilled an attitude of protecting the organization against turnover and stagnation, since the same interviewees highlighted the importance of change in work roles.

"there is this thing called the half-life of a manager. In five years, their efficiency will halve. In five years, they get stuck in routines and stop creating new things, so it is also not good to have one person in the same position as long as possible and in that way be efficient"

Perhaps nowadays the company has learned from the painful process of replacing the retired manager and foster the attitude described in the latter quote of need for change in manager roles regularly.

The first risk linked to knowledge loss because of turnover is that knowledge is lost and not usable for the benefit of the organization. The second risk linked to turnover is too little of it, which can lead to stagnation and knowledge decay. Even if people stay in the same organization, their role should be renewed every now and then, so that they are "forced" to learn new things and teach things to others. In the case of the retiring manager, it may be that the organization suffers from both: first, the manager being stuck in their routines for a long time, and thus declining in their creativity and productivity, and second, the manager leaving and causing a lot of effort to transfer their knowledge before retirement.

The risk of a leaving employee is easier to tackle if there is time to prepare and the retiring person is available for knowledge transfer. Sometimes, however, employees are lost unexpectedly to accidents or illness, which happened in another company.

"One very experienced designer died. We have missed the knowledge that he had. At least you realize [the value] when you don't have [the knowledge] anymore."

In a case like this, if the valuable knowledge has not been identified, and the presence of the people has been taken for granted, there is little that can be done as a reaction. Proactive knowledge identification and transfer is the only means of mitigating risks like this, and hence, learning from the incident for future is essential.

5. Discussion of results

The analysis of our four cases shows that knowledge risk incidents can have serious effects for companies and that both preventive and reactive measures are justified. Even if none of the four companies got bankrupt, the effects are serious. In the spill-over case the owner made very clear estimations about the loss, but at the same time also highlights that his strict knowledge protection measures of the last four years secured additional revenues. Thus, for him the knowledge protection measures clearly paid off and he could assign 500.000€ revenue to his measures per year.

For the violation of trust case, the interviewee described the incident as very critical as it affected a major product of the company. Even if he could not quantify the loss, he made clear that this was an existential threat. This is like the turnover case, in which the impact is clear and serious but difficult to quantify. In the immature idea case, a business opportunity is lost. The risk is more focused on future business than on the current business and thus difficult to quantify. Despite the challenge, the interviewee made clear that this was an important business opportunity and that he should have given more attention to protection.

A second important insight of our analysis is that it is important to know the potential threat, or for the first three cases, to know the potential attacker well. The ancient war-related proverb, made famous by Sun Tzu, "know yourself, know your enemy" is thus highly relevant also for dealing with knowledge risks. In the spill-over case, the owner had a very clear idea who would be the attacker and he designed the measures accordingly. One of the main reasons for successfully hiding the knowledge for four years was the adept competitor analysis.

In contrast to this, not understanding the potential attacker caused the incidents in the violation of trust as well as the immature idea case. In the violation of trust case the company simply did not anticipate that their big customer would forward the knowledge to a Chinese competitor. Similar in the immature idea case, here the interviewee did not expect that his conversation partner would exploit the idea. In both cases, the interviewee said that a more rigorous analysis of their sharing partners could have helped to avoid these incidents, which is in line with literature [e.g. 29, 41]. However, the emphasis here is on the word could. In addition to helping in preventing the incidents from happening, analyzing the situation beforehand to create a plan in case the spillover or violation of trust happens, might have helped the organizations with their recovery.

In the turnover case, it seems clear that knowing the threat in advance allows to take suitable countermeasures, i.e. distributing the critical knowledge to other employees. Retirement as an unavoidable knowledge loss incident has also received a lot of attention in the literature [e.g. 8, 18]. Despite this attention, and an older case, we argue that acknowledging this threat could be done more promptly in many organizations. Although there are literature that discuss the importance of threat assessment also in connection with knowledge [8, 15, 16, 41], the term threat is often linked to sources that come from outside the organization. In case of turnover, the threat and "attack" comes from inside.

Although natural and unavoidable, employee turnover needs to be also seen as a threat, so that proper measures and reaction plans can be put in place.

Our cases also show that knowing the competitors and taking preventive measures does not always help to avoid a knowledge risk incident at all. In the spill-over case the owner was fully aware that he will not be able to protect the knowledge forever, but the prevention of the spillover for two years was a success for him. Hence, delaying knowledge risk incidents can be a reasonable goal for knowledge protection strategy, as is also discussed in literature [e.g. 1].

The goal of delaying as the goal of knowledge protection is important as it also influences the design of the protection measures. Thus, not only the knowledge itself, the threat and the potential attacker are important decision variables, but also the protection extent and the protection period. Regarding the knowledge itself, the immature idea case clearly showed that the suitability of protection measures depends on the maturity of knowledge. As immature knowledge is less complex, it is more challenging to leave details out as a protection strategy [3]. Hence, the analysis of the communication partner is even more important and sharing with less-proximate sharing partners is one suitable protection strategy for immature knowledge [28].

Our analysis of the related work showed that knowledge risk and protection literature mainly focus on preventive strategies and measures so far. Our four cases also provided evidence for the suitability of this approach. However, the analysis of all four cases also shows a need for reactive measures having a clear after-incident strategy and a plan if a knowledge risk incident happens.

In the turnover case, the interviewee reported about the frustrating experience of managing the knowledge loss and how his company was now damned to reactions to the competitor instead of setting proactive actions. In this case it became also clear that only a good strategy to block the sequences of the unwanted knowledge spillover prevented the company from really serious consequences.

In the spillover and the immature idea case, both had no reaction plan. For the spillover case this was not intended as delaying was the goal. Nevertheless, it is not clear if countermeasures would have additionally delayed the knowledge assimilation by competitors. For the immature idea case also no strategy or plan was in place and thus the competitor could exploit the idea easily. Even if the knowledge protection literature rarely discusses “reaction plans” for incidents, this is a standard procedure in other related domains [34] and thus application of the incident planning approach to knowledge risks could draw on these domains.

In all four cases, the interviewees critically reflected the cases with us in the interviews. But in none of the four companies was a systematic “learning from failure” procedure in place. In the turnover case and the immature knowledge case, the interviewees pointed very clearly out that they learned from the incident and that they will draw conclusions from it. In the turnover case it became clear that lessons learned were also communicated within the organization, but it is not clear if concrete measures or organizational practices are implemented in response.

Based on our insights we argue for a systematic investigation of knowledge risk incidents in research as well as practice. Based on our secondary analysis of interviews we were able to get new insights and it seems that knowledge protection research would benefit from more research in this direction. Regarding the knowledge protection practice, we are convinced that organizational knowledge protection should also include a systematic approach to learn from knowledge risk incidents. Related research shows that organizational losses from incidents can be reduced dramatically by focusing on the learning cycle from incidents [7]. Hence, knowledge protection frameworks and practices should be extended in this regard.

6. Conclusion and Outlook

As a summary of the above analysis four main conclusions are drawn:

1.) Knowledge risk incidents have a negative impact on businesses, and thus preventive and reactive measures are clearly justified. Further research on real incidents could strengthen this justification.
2.) Knowing the potential attacker and their motivations is important for employing successful preventive knowledge protection measures. Competitor analysis thus becomes also a tool for knowledge risk management, not just business management in general.
3.) Some knowledge risk incidents are not preventable, they can be merely delayed. A knowledge protection strategy focusing on delaying knowledge spillovers can be economically justifiable.
4.) Planning for knowledge risk incidents is important, so that organizations can recover faster. One part of these plans should be a process of learning from the incident, for the further improvement of the knowledge protection measures.

Based on our findings from the analysis of the four cases, we argue for more research on concrete knowledge incidents, preventive knowledge protection measures and a research culture focusing on learning from failure instead of repressing or forgetting incidents. This seems especially relevant in regard to emerging knowledge risks in data-centric collaborations [16, 21].

One possible avenue for pursuing this research is to locate organizations that have faced knowledge risk incidents and study their responses to the incidents and their learning from them. Although locating such organizations may be difficult, the mandatory reporting of privacy incidents and the response to them in Europe may provide openings to locate potential organizations. Based on this research, it seems promising to develop reactive measures as part of knowledge protection frameworks.

References

[1] Ahmad, A., R. Bosua, and R. Scheepers, "Protecting organizational competitive advantage: A knowledge leakage perspective", *Computers & Security 42*, 2014, pp. 27–39.

[2] Albrechtsen, E., and J. Hovden, "The information security digital divide between information security managers and users", *Computers & Security 28*(6), 2009, pp. 476–490.

[3] Barnes, S.-A., J. Bimrose, A. Brown, et al., "Knowledge maturing at workplaces of knowledge workers: Results of an ethnographically informed study", *Proceedings of 9th International Conference on Knowledge Management and Knowledge Technologies., Graz, Austria,* 2009, 14–27.

[4] Beazley, H., J. Boenisch, and D. Harden, *Continuity Management: Preserving Corporate Knowledge and Productivity When Employees Leave*, Wiley, 2007.

[5] Belsis, P., S. Kokolakis, and E. Kiountouzis, "Information systems security from a knowledge management perspective", *Information Management & Computer Security 13*(3), 2005, pp. 189–202.

[6] Botha, J., and R. Von Solms, "A cyclic approach to business continuity planning", *Information Management & Computer Security 12*(4), 2004, pp. 328–337.

[7] Cooke, D.L., and T.R. Rohleder, "Learning from incidents: from normal accidents to high reliability", *System Dynamics Review 22*(3), 2006, pp. 213–239.

[8] Durst, S., "How far have we come with the study of knowledge risks?", *VINE Journal of Information and Knowledge Management Systems 49*(1), 2019, pp. 21–34.

[9] Durst, S., and M. Zięba, "Knowledge risks - towards a taxonomy", *International Journal of Business Environment 9*(1), 2017, pp. 51–63.

[10] Durst, S., and M. Zieba, "Mapping knowledge risks: towards a better understanding of knowledge management", *Knowledge Management Research & Practice 17*(1), 2019, pp. 1–13.

[11] Edmondson, A.C., "Strategies of learning from failure.", *Harvard business review 89*(4), 2011, pp. 48–55, 137.

[12] Elliott, K., A. Patacconi, J. Swierzbinski, and J. Williams, "Knowledge Protection in Firms: A Conceptual Framework and Evidence from HP Labs", *European Management Review 16*(1), 2019, pp. 179–193.

[13] Fortune, J., and G. Peters, *Learning from failure - The systems approach*, Wiley, Chichester, UK, 1995.

[14] Holsapple, C.W., and K.D. Joshi, "An investigation of factors that influence the management of knowledge in organizations", *The Journal of Strategic Information Systems 9*(2), 2000, pp. 235–261.

[15] Ilvonen, I., J.J. Jussila, and H. Kärkkäinen, "Towards a Business-Driven Process Model for Knowledge Security Risk Management:: Making Sense of Knowledge Risks", *International Journal of Knowledge Management 11*(4), 2015, pp. 1–18.

[16] Ilvonen, I., S. Thalmann, M. Manhart, and C. Sillaber, "Reconciling digital transformation and knowledge protection: a research agenda", *Knowledge Management Research & Practice 16*(2), 2018, pp. 235–244.

[17] Jafari, M., J. Rezaeenour, M.M. Mazdeh, and A. Hooshmandi, "Development and evaluation of a knowledge risk management model for project-based organizations: A multi-stage study", *Management Decision 49*(3), 2011, pp. 309–329.

[18] Jennex, M., "A proposed method for assessing knowledge loss risk with departing personnel", *VINE 44*(2), 2014, pp. 185–209.

[19] Jennex, M., and A. Durcikova, "Integrating IS Security with Knowledge Management: Are We Doing Enough?", *International Journal of Knowledge Management (IJKM) 10*(2), 2014, pp. 1–12.

[20] Johnson McManus, D., and C. Snyder, "Knowledge management: the missing element in business continuity planning", 2004, pp. 79–91.

[21] Kaiser, R., S. Thalmann, V. Pammer-Schindler, and A. Fessl, "Collaborating in a Research and Development Project: Knowledge Protection Practices applied in a Co-opetitive Setting", *Proceedings of the 10th International Conference on Practical Knowledge Management, Lecture Notes on Informatics, Potsdam, Germany*.

[22] von Krogh, G., "How does social software change knowledge management? Toward a strategic research agenda", *The Journal of Strategic Information Systems 21*(2), 2012, pp. 154–164.

[23] Levallet, N., and Y.E. Chan, "Organizational knowledge retention and knowledge loss", *Journal of Knowledge Management*, 2019.

[24] Levy, M., C. Loebbecke, and P. Powell, "SMEs, co-opetition and knowledge sharing: the role of information systems", *European Journal of Information Systems 12*(1), 2003, pp. 3–17.

[25] Lin, T.-C., C.L. Chang, and W.-C. Tsai, "The influences of knowledge loss and knowledge retention mechanisms on the absorptive capacity and performance of a MIS department", *Management Decision 54*(7), 2016, pp. 1757–1787.

[26] Loebbecke, C., P.C. van Fenema, and P. Powell, "Managing inter-organizational knowledge sharing", *The Journal of Strategic Information Systems 25*(1), 2016, pp. 4–14.

[27] Manhart, M., and S. Thalmann, "Protecting organizational knowledge: a structured literature review", *Journal of Knowledge Management 19*(2), 2015, pp. 190–211.

[28] Manhart, M., S. Thalmann, and R. Maier, "The Ends of Knowledge Sharing in Networks: Using Information Technology to Start Knowledge Protection", *ECIS 2015 Completed Research Papers*, 2015.

[29] Marabelli, M., and S. Newell, "Knowledge risks in organizational networks: The practice perspective", *The Journal of Strategic Information Systems 21*(1), 2012, pp. 18–30.

[30] Massingham, P., "Knowledge risk management: a framework", *Journal of Knowledge Management*, 2010.

[31] Massingham, P.R., "Measuring the impact of knowledge loss: a longitudinal study", *Journal of Knowledge Management 22*(4), 2018, pp. 721–758.

[32] Padyab, A.M., T. Päivärinta, and D. Harnesk, "Genre-Based Approach to Assessing Information and Knowledge Security Risks", *International Journal of Knowledge Management (IJKM) 10*(2), 2014, pp. 15.

[33] Perrott, B.E., "A strategic risk approach to knowledge management", *Business Horizons 50*(6), 2007, pp. 523–533.

[34] Phillips, R., and B. Tanner, "Breaking down silos between business continuity and cyber security", 2019. https://www.ingentaconnect.com/content/hsp/jbcep/2019/00000012/00000003/art00004

[35] Reimsbach, D., and R. Hahn, "The Effects of Negative Incidents in Sustainability Reporting on Investors' Judgments–an Experimental Study of Third-party Versus Self-disclosure in the Realm of Sustainable Development", *Business Strategy and the Environment 24*(4), 2015, pp. 217–235.

[36] Sarigianni, C., S. Thalmann, and M. Manhart, "Knowledge Risks of Social Media in the Financial Industry", *International Journal of Knowledge Management (IJKM) 11*(4), 2015, pp. 19–34.

[37] Szabo, V., and V. Strang, "Secondary Analysis of Qualitative Data", *Advances in Nursing Science 20*(2), 1997, pp. 66–74.

[38] Thalmann, S., and I. Ilvonen, "Balancing Knowledge Protection and Sharing to Create Digital Innovations", In *Knowledge Management in Digital Change*. Springer, Cham, 2018, 171–188.

[39] Thalmann, S., and M. Manhart, "Enforcing organizational knowledge protection: an investigation of currently applied measures", *Seventh (pre-ICIS)*

Workshop on Information Security and Privacy (WISP), Milan, Italy, 2013.

[40] Thalmann, S., M. Manhart, P. Ceravolo, and A. Azzini, "An Integrated Risk Management Framework: Measuring the Success of Organizational Knowledge Protection", *International Journal of Knowledge Management (IJKM) 10*(2), 2014, pp. 28–42.

[41] Trkman, P., and K.C. Desouza, "Knowledge risks in organizational networks: An exploratory framework", *The Journal of Strategic Information Systems 21*(1), 2012, pp. 1–17.

[42] Väyrynen, K., R. Hekkala, and T. Liias, "Knowledge Protection Challenges of Social Media Encountered by Organizations", *Journal of Organizational Computing and Electronic Commerce 23*(1–2), 2013, pp. 34–55.