Journal of Knowledge Management

Protecting organizational knowledge: a structured literature review

Markus Manhart Stefan Thalmann

Protecting organizational knowledge: a structured literature review

Markus Manhart and Stefan Thalmann

Markus Manhart is a Researcher and Stefan Thalmann is an Assistant Professor both are based at Information Systems, Production and Logistics Management, University of Innsbruck, Innsbruck, Austria.

Abstract

Purpose – *The purpose of this paper is to investigate pertinent knowledge protection literature. At the same time, however, knowledge protection is often a neglected or underdeveloped area. This is all the more concerning as knowledge protection plays an essential part in preserving an organization's competitive advantage. Despite the recognition of this issue by scholars, the knowledge management literature has so far tended to concentrate on the facilitation of knowledge sharing rather than on knowledge protection.*

Design/methodology/approach – *In this paper, the authors present the results of a structured literature review undertaken to investigate the current state of research on knowledge protection. The paper identifies core domains in knowledge protection literature, discusses theoretical perspectives and research methods, sheds light on the role of the information technology (IT) artefact in knowledge protection research and develops a portfolio of knowledge protection measures.*

Findings – *In this paper, 48 papers were analyzed by taking five analytical dimensions into account: research domains, research methods and models, the role of the IT artefact, theoretical views and measures to enforce knowledge protection. Based on the discussion of the results, promising avenues for further research were identified and a research agenda was proposed. The authors argued for more research on the protection of tacit knowledge, more in-depth empirical investigations, more research on IT support and a stronger consideration of theories in knowledge protection research, as well as research on how organizations could build a strategy of knowledge protection.*

Research limitations/implications – *Tacit knowledge, as well as informal alliances or (social) networks, is under-researched so far. Knowledge protection phenomena need to be investigated in depth to test the assumptions stated in many conceptual papers. IT artefacts should be developed and evaluated. More theory-based research and overarching frameworks or strategies for knowledge protection need to be developed.*

Practical implications – *In this paper, a portfolio of knowledge protection measures was developed, which might be of particular interest for practitioners. Further, the paper provides a good overview of the current state of practice regarding knowledge protection.*

Originality/value – *So far, there is no structured literature available focussing on the topic of knowledge protection.*

Keywords *Literature review, Knowledge protection, Intellectual property, Knowledge security, Protection measures*

Paper type *Literature review*

1. Introduction

It is no secret that organizations rely heavily on information systems (IS) and that widely publicized security breaches have fuelled organizational awareness of the need to protect themselves against the commercial consequences of knowledge theft (Dhillon and Torkzadeh, 2006). Subsequently, investment in data protection has also risen, with companies spending significant amounts of money and resources to, for example, adopt frameworks such as COBIT and engage with auditors in the verification of protection measures (Bachlechner *et al.*, 2014). Paradoxically, while knowledge is considered as an organizational asset that must be protected, and despite empirical research showing that

Received 20 May 2014
Revised 9 September 2014
12 September 2014
Accepted 18 September 2014

The research leading to the presented results was partially funded by the European Commission under the 7th Framework Programme (FP7) and Learning Layers (Project no. 318209).

DOI 10.1108/JKM-05-2014-0198

“The literature on knowledge protection mostly fails to consider the IT artefact as it originates in the research field of strategic management.”

successful knowledge protection significantly enhances organizational performance (Lee *et al.*, 2007), knowledge managers still seem to pay little attention to security issues in their jobs (Asllani and Luthans, 2003). Empirical research has revealed a number of barriers to knowledge protection measures, particularly from a knowledge management (KM) perspective. This includes the consideration that knowledge protection is frequently considered as a barrier to knowledge sharing (Khamseh and Jolly, 2008), or that it is often narrowly understood as the management of digital rights and thus seen as part of the management of intellectual property rights (IPR) (Lee and Yang, 2000). Additionally, it is found that firms consider their intellectual capital to be mainly residing in their employee’s brains (Chan and Lee, 2011) and although such “tacit knowledge” is often difficult to document, it is a valuable source of competitive advantage (Norman, 2002).

Neglecting knowledge protection can cause the replication of ideas by external organizations and hence hinder the exploitation of innovations (Cheung *et al.*, 2012). Knowledge leakage is also known to be able to cause reputational damage, loss of revenue and productivity (Ahmad *et al.*, 2014). Hence, finding a balance between protecting and sharing knowledge is crucial to solving the boundary paradox (Norman, 2002).

The challenge of finding a balance between knowledge sharing and knowledge protection is further exacerbated by recent developments in the field of social media and mobile technologies, which generally facilitate knowledge sharing (Bruck *et al.*, 2012). To overcome this challenge, organizations should apply a holistic risk management approach that establishes a sustainable and traceable link between high-level knowledge protection requirements and their concrete implementation (Thalmann *et al.*, 2014). However, it would appear that many organizations seem to lack a clear knowledge protection strategy in the first place that would enable them to tackle knowledge protection in a systematic way (Alstete, 2003; Olander *et al.*, 2011; Ahmad *et al.*, 2014).

This paper aims to review the current research on knowledge protection. The authors are specifically interested in identifying the research areas covered, the methods and models applied, the role of the information technology (IT) artefact and the theoretical perspectives adopted by scholars, as well as in measures proposed to implement knowledge protection requirements in practice. The paper is structured as follows: first the authors describe the related work to define the term knowledge protection. This is followed by an outline of the procedure adopted in the literature review and the presentation and discussion of the results. Finally, a research agenda based on the findings is proposed. The paper concludes with a short summary.

2. Related work

Knowledge is a multifaceted term whose definition varies from discipline to discipline and even between individual domains (Maier, 2007). Computer sciences distinguish between data, information and knowledge (Alavi and Leidner, 2001), with data considered as consisting of raw and unanalyzed elements such as symbols and requires input into an interpretation process, whereas information is related to meaning and thus results from the aggregation of data (Trkman and DeSouza, 2012). Knowledge in this perspective is characterized by its relationship to and impact on the user, as it is subject to his or her interpretation and application (Maier *et al.*, 2009), thus providing the necessary context for the interpretation of data and information (Trkman and DeSouza, 2012). Theories of knowledge furthermore differentiate between tacit and explicit knowledge (Nonaka, 1994; Chan and Lee, 2011). Tacit knowledge is highly personal and rooted in actions; it consists of mental models, beliefs and individual perspectives which makes it difficult for the person to articulate it. This contrasts with explicit knowledge, such as a document for example, which by being formalized and systematic can easily be communicated and shared within communities (Olander *et al.*, 2011).

KM is still a young research field comprising many different definitions of the term (Maier, 2007). In the present work, the authors share the views of Schultze and Leidner (2002) who consider KM as "the generation, representation, storage, transfer, transformation, application, embedding, and protecting of organizational knowledge". While Bloodgood and Salisbury (2001) designate knowledge protection, alongside knowledge creation and knowledge transfer, as one of the three central KM strategies for organizations to gain a competitive advantage, the KM literature overall deems knowledge protection to be the least important success factor for KM (Jennex and Olfman, 2005). Current research therefore suggests that the complex issue of knowledge protection is often overlooked at the management level and the responsibility for it is left with the knowledge "owners" (Ahmad *et al.*, 2014). This also highlights the need for knowledge protection to be integrated into a holistic KM strategy with strategic protection goals that can be linked to operational practices (Pawlowski *et al.*, 2014).

Knowledge protection focusses on:

- the prevention of unwanted knowledge spillovers, which focus on leakage of knowledge to non-authorized people (Ahmad *et al.*, 2014);
- the reduction of knowledge visibility which is concerned with the observability of knowledge by externals (Lee *et al.*, 2007); and
- the prevention of knowledge loss which focuses on unavailable employees, e.g. those leaving or retiring (Jennex and Durcikova, 2013).

Knowledge protection has to be differentiated from the wider concept of knowledge security which is concerned with both external and internal confidentiality, integrity and availability of knowledge (Ilvonen, 2013), and can be considered as the intersection of KM and information security (DeSouza, 2006). Occupying this perspective, the authors argue that organizations should apply a security perspective on knowledge transfer (Gerber and Von Solms, 2005). In information security, security requirement analysis is a top–down process which takes into consideration business, legal and regulatory requirements, as well as infrastructure risks (Gerber and von Solms, 2001). Applied to the knowledge dimension, this includes "technical, administrative and managerial controls" and "a formal plan that contains policies stating how the organization intends to implement security", as well as "education and awareness" (Jennex and Zyngier, 2007).

One major issue for firms is finding a balance between sharing and protecting knowledge. Involvement in strategic alliances requires firms to access external knowledge while simultaneously protecting internal knowledge (Quintas *et al.*, 1997; Norman, 2002). This so-called boundary or learning paradox has been subject to many investigations without having been solved yet, but a satisfactory solution could lead to more effective organizational partnerships (Jordan and Lowe, 2004).

> **"The vast majority of papers failed to present their insights in a specific theoretical framework. This shows that knowledge protection is still in its infancy."**

There are many reasons why knowledge protection is considered as especially challenging:

- knowledge-based resources are drivers for other resources, consume a lot of resources to develop and are difficult to substitute (DeSouza, 2006);
- the protection of explicit knowledge remains hard to achieve, as property rights are very costly to write and enforce (Chan and Lee, 2011); and
- although the security literature provides approaches towards awareness training, as well as access and authorization schemes, this does not fully cover the question of *how to protect knowledge in people's brains* (DeSouza, 2006).

Tacit knowledge is sticky and complex (Nelson and Winter, 1982), and, as it eludes observation, it cannot be easily codified or articulated (Nonaka and Takeuchi, 1995) – this makes protection challenging. However, tacit knowledge is particularly important when it is considered by some as the main source of competitive advantage (Norman, 2002). Tacit knowledge must therefore be articulated, verbalized and structured if it is to become information. Finally, data are obtained after tacit knowledge has been represented and interpreted (Tuomi, 1999). Higher formalized structures facilitate the application of information security approaches. The more a document can be described and classified, the better it can be protected, but, at the same time, this makes its observation by third parties easier.

In the literature and in practice, much attention is devoted to data and information security; however, beyond the protection of explicit knowledge through patents, copyrights and trade secrets, the development of holistic approaches towards knowledge protection is, for the most part, neglected (Väyrynen *et al.*, 2013). Key to successful approaches to knowledge security would be the proper planning of systematic protection, both of explicit and tacit knowledge, as well as finding a balance between sharing and protecting. If this can be better understood by organizations, new strategies for knowledge protection stand a greater chance of being explored (Alstete, 2003).

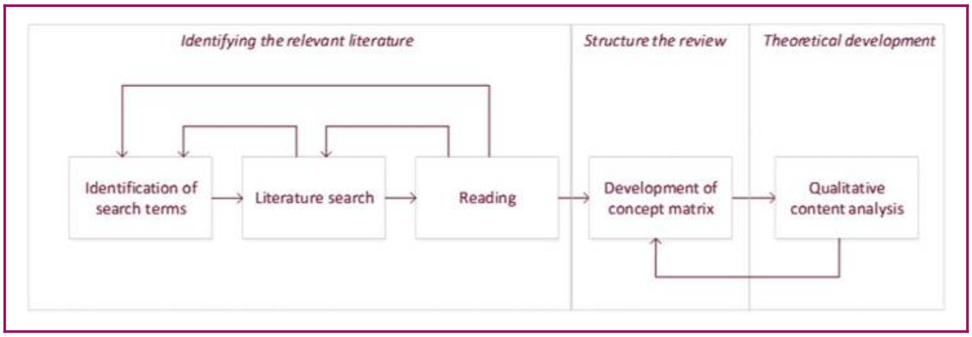
3. Methodology

The authors followed the approach proposed by Webster and Watson (2002) for conducting a structured literature review and applied the proposed three-step procedure:

1. Identifying the relevant literature.
2. Structuring the review.
3. Contributing to theory.

The procedure with its three steps is illustrated in Figure 1 and is described in the following sections.

Figure 1 Procedure of the literature review


Identifying the relevant literature
Structure the review
Theoretical development
Identification of search terms
Literature search
Reading
Development of concept matrix
Qualitative content analysis

“Informal collaborations between organizations, such as communities of practice, received little attention so far.”

3.1 Identifying the relevant literature

To identify the relevant literature, the authors started with a building-blocks approach (Rowley and Slack, 2004), first determining ten search terms combined with the term knowledge: protection, security, guard, defence, save, control, audit, privacy, loss and risk. All terms have been truncated according to Boolean rules of the different search hosts: Ebsco, Jstor, Sciverse and Google Scholar. As a starting point, the authors decided to query the hosts for pertinent and high-quality journals: 15 journals with a specific KM and 10 with a security management focus, as well as the AIS senior scholars’ basket of 8. The reason behind this selection was the focus on confidentiality of knowledge protection in the authors’ own research, which is why information security and top-IS journals were also expected to yield valuable resources. Conducting a title and keyword search using the defined search terms returned 51 articles. The authors scanned the abstracts of these papers to evaluate their suitability for our purpose. Articles that focussed on knowledge *about* protection instead of protection *of* knowledge were excluded. The same held for articles that investigated knowledge that lies beyond the scope of organizations, such as cultural heritage. These criteria match what Webster and Watson (2002) refer to as *tone*, in that they are objective by not systematically excluding papers a priori and according to quality criteria. This process resulted in 22 papers that were considered as useful in accordance with the aforementioned criteria.

To grasp the whole body of knowledge, the authors subsequently analyzed each of the papers in depth and conducted a backward and forward search (Webster and Watson, 2002). Subsequently, a second iteration of literature identification was performed which incorporated books, conference proceedings and journals with other foci, such as strategic management. By doing so, the authors encountered additional search terms in papers related to the topic of knowledge protection, such as IPR, intellectual capital appropriability, spillovers and innovation. With this approach, the authors identified an additional 26 suitable papers and ended up with a total of 48 papers in the set.

3.2 Structuring the review

In a second step, the authors structured this review in a concept-centric way. Therefore, a concept matrix was developed (Webster and Watson, 2002). In addition to the concepts being discussed in the papers (e.g. measures of knowledge protection, methods applied and IT artefacts proposed), the authors also added fields proposed by DeLone and McLean (1992) to the matrix that described the articles in general: short summary, type of article, research question, theories and conceptual views obtained.

3.3 Theoretical development

To identify patterns, the authors adopted an informed-inductive coding approach described by Patton (2002). The two authors coded the papers using ATLAS TI and repeatedly performed the qualitative content analysis (Patton, 2002) until patterns amongst the papers became apparent. This also led to a gradual refinement of the concept matrix. The authors structured and analyzed the papers in the set according to the following dimensions:

- *Domains*: Building on the study by Seidel *et al.* (2010), the authors aggregated the content discussed in the set of papers to core domains of discussions covered in the knowledge protection literature. The authors considered this dimension as an essential part of providing the reader with an overview of the topics covered.

- *Research methods and models*: The authors outline the research methods applied and research models developed, including a description of the constructs and the relationship between them. The authors borrow this dimension from Seidel *et al.* (2010) who also argued that both research models and research methods are crucial dimensions to identifying further research avenues in terms of recently ignored methods or (in)dependent variables.
- *Role of IT artefact*: The authors analyzed the papers according to whether and how they treat the IT artefact to investigate the status of the current IT support in current knowledge protection research. Orlikowski and Iacono (2001) identified five views on the IT artefact in the IS literature, i.e. the tool, the ensemble, the nominal, the computational and the proxy view.
- *Theoretical perspectives*: The authors describe the theoretical lenses from which knowledge protection is discussed and how the different papers contributed to them. This is concluded with a short statement of how scholarly work contributes to the body of literature, ranging from explanatory, predictive statements, to testable statements (Gregor, 2006).
- *Knowledge protection measures*: The authors describe the measures for knowledge protection discussed in the literature referring to different levels of organizational protection, i.e. risk management goals, knowledge protection objectives and knowledge protection mechanisms. By incorporating this dimension, the authors are able to identify on which of these levels organizations can protect their knowledge and to investigate whether the literature provides holistic approaches linking the different levels (Thalmann *et al.*, 2014).

4. Discussion of results

In the following sections, we structure the discussion of results according to the analytical dimensions:

- research domains;
- research methods and models;
- the role of IT artefact;
- theoretical perspectives; and
- measures to enforce knowledge protection.

4.1 Research domains

The authors identified three different domains of research on knowledge protection. Scholars are mainly concerned with the prevention of knowledge spillovers and leakage in organizational alliances, the relationship of spillover and leakage prevention to competitive advantage and the relationship of spillover and leakage prevention to intellectual capital. The second main stream focusses on knowledge retention and the third main stream on the prevention of knowledge loss.

"The main focus in the current literature is on the protection of explicit knowledge whilst the tacit knowledge dimension is by and large neglected."

4.1.1 Knowledge protection in alliances. Scholars focussing on this domain are basically concerned with the so-called boundary paradox presented by organizations wanting to access external knowledge and, at the same time, protect internal knowledge (Quintas *et al.*, 1997; Norman, 2001; Jordan and Lowe, 2004). Here, researchers tried to formalize this dilemma (Ding and Huang, 2010), and they investigated the challenge of reaching both goals for organizations (Kale *et al.*, 2000). Mayer (2006) investigated alliance outcomes and Lee *et al.* (2007) discussed how knowledge protection influences alliance outcomes (Norman, 2004) and how learning intent, opportunities to learn and a firm's ability to learn influence alliance outcomes (Norman, 2004).

4.1.2 Securing intellectual capital. Papers dealing with this topic frequently discuss the effectiveness of measures to protect IPR, i.e. patents, trade secrets, copyrights and trademarks (Hannah, 2005; Hertzfeld *et al.*, 2006; Arundel, 2001). Scholars also focus on firms' choice of IPR protection mechanisms (Cohen *et al.*, 2000; Encaoua *et al.*, 2006), as well as on how important organizations consider formal protection methods (Howells *et al.*, 2003). IPR measures are well known and established for formal and mature knowledge (Link and Ruhm, 2011). However, the challenge is how to apply these measures to more immature and informal knowledge and to propose suitable measures. The selection of collaboration partners considering IPR characteristics is another domain that has been investigated (Li *et al.*, 2008).

4.1.3 Knowledge protection to maintain competitive advantage. Here, scholars investigated the relationship between different protection approaches and competitive advantage. Liebeskind (1996) argues that the protection of knowledge is central to achieving and maintaining a competitive advantage. Authors focussed on the investigation of factors like trust (Norman, 2002), sector or firm size (Brouwer and Kleinknecht, 1999) as influencing the protection behaviour of organizations. Another important focus in this area is the risk of using social media and how this might jeopardize competitive advantage (Väyrynen *et al.*, 2013). Overall, it is stressed that maintaining competitive advantage depends on adequate prevention of unwanted spillovers. Intersectional work investigates the effectiveness of IPR measures and sources of competitive advantage, i.e. strategies against economic espionage (Snyder and Crescenzi, 2009) or on the selection of IPR protection mechanisms (Amara *et al.*, 2008; Harabi, 1995).

4.1.4 Knowledge protection to prevent knowledge loss. Papers dealing with this topic focus on the risk of knowledge loss caused by employees leaving the organization and discuss preventive measures or frameworks. Knowledge loss, complementary to knowledge spillover, is mostly investigated from a human resource perspective (Jennex and Durcikova, 2013; Boyles *et al.*, 2009).

4.2 Research methods and models

In this section, the authors set out to describe different types of methods applied and research models used in the set of papers. In total, 26 qualitative and 17 quantitative, as well as 5 mixed method studies have been found. The results are summarized in Table I.

4.2.1 Qualitative methods. The authors counted 26 papers using qualitative approaches, of which 16 papers are conceptual and 8 papers are broadly explorative or case studies.

4.2.1.1 Conceptual papers. Amongst a total of 18 papers, eight propose frameworks for risk management or knowledge protection (Trkman and DeSouza, 2012; Boyles *et al.*, 2009; Teece, 1986; Snyder and Crescenzi, 2009; Jennex and Durcikova, 2013; Aljafari and Sarnikar, 2009; Baughn *et al.*, 1997; Randeree, 2006); eight make propositions or recommendations on knowledge protection issues for researchers or practitioners (Upadhyaya *et al.*, 2011; Bertino *et al.*, 2006; Liebeskind, 1996, 1997; DeSouza, 2006; Encaoua *et al.*, 2006; Bloodgood and Salisbury, 2001; Lucas, 2010); and two propose research models, one on securing KM strategy (Urcuyo and Kunnathur, 2002) and the other on success and failure factors (Neville *et al.*, 2003).

Table I Methods used

Method	*No. of papers*
Qualitative	
Conceptual	18
Case studies	5
Qualitative interviews	3
Quantitative	
Questionnaire surveys	5
Database queries	10
Experiment	1
Formal model	1
Mixed method approaches	5
Sum of papers	48

Overall, the conceptual papers are mostly prescriptive and focus on making recommendations or providing guidance frameworks. The research models mostly have an informative and less formal character and are not empirically validated, which is an indicator for low maturity in the research field. To strengthen the robustness of research in this field, future research should aim for a stronger formalization, validation of propositions and provide decision support.

4.2.1.2 Empirical approaches. Eight papers performed qualitative research by means of case studies or explorative approaches. For case studies, the range of qualitative data collection was much broader, and it comprised multiple converging sources of data and collection methods with a sample collected by means of semi-structured interviews complemented by document analysis (Jennex and Zyngier, 2007; Jordan and Lowe, 2004; Chan and Lee, 2011) and on-site observations (DeSouza and Vanapalli, 2005). The exploratory papers comprised data collection methods including semi-structured interviews, online discussion boards (Alstete, 2003) and action research (Baughn *et al.*, 1997; Väyrynen *et al.*, 2013; Jennex, 2009) action research.

Summing up, the qualitative studies were mainly of an exploratory nature, scoping the fields of research. The broad use of data collection and analysis methods enabled the phenomenon of knowledge protection to be investigated in a specific organizational context. However, more in-depth investigations in the form of observation studies or ethnographies are missing. Due to the tacit dimension of knowledge and the importance of motivations and attitudes, such in-depth investigations would seem particularly appropriate, and are therefore recommended by the authors.

4.2.2 Quantitative approaches. The authors counted 17 papers that used quantitative approaches, of which 5 were quantitative empirical studies, 10 were quantitative statistical tests relying on existing surveys stored in databases, one used experiments and the another develops a mathematical model.

The five *quantitative empirical studies* undertook questionnaire surveys to investigate three different perspectives: testing hypotheses:

1. About knowledge protection in alliances (Lee *et al.*, 2007).
2. On factors that influence the organizational knowledge protection behaviour (Norman, 2002; Kale *et al.*, 2000).
3. On the organizational impact of knowledge protection (Norman, 2004) or organizational effectiveness (Gold *et al.*, 2001).

Ten papers *quantitatively analyzed existing data stored in databases.* Here the focus is on analyzing contracts between alliances, as well as on survey data on innovation activities. Six out of ten papers use protection behaviour-related constructs as dependent variable, e.g. organizations' selection of measures, to test how knowledge protection behaviour is influenced by factors like firm size (Brouwer and Kleinknecht, 1999), industry sector (Brouwer and Kleinknecht, 1999; Harabi, 1995; Amara *et al.*, 2008), knowledge type (Amara *et al.*, 2008) and individuals' professional background (Link and Ruhm, 2011), as well as innovation expenditures and multi-nationality of firms (de Faria and Sofka, 2010).

One paper out of 18 used a *quantitative experiment* to validate a knowledge protection prototype in two community software development cases measuring protection success with Key Performance Indicators (Zhou and Liu, 2010). Another paper developed a quantitative game theoretical model to formalize the boundary paradox (Ding and Huang, 2010).

Scholars investigated the relationships in the context of formal alliances. Informal associations, such as networks, however, have not yet formed the object of any investigations so far. Moreover, while there is a strong focus on IPR in terms of documented process and product knowledge, the relationship of protection mechanisms for tacit knowledge on various constructs like partner selection or alliance outcomes is mostly neglected. Another issue is the small variety of industry sectors. More knowledge-intensive industries like finance or consulting should also be taken into account. Another issue is the operationalization of protection behaviour as the independent variable. Most studies investigate the selection decisions of whether protection measures are undertaken. Last but not least, the authors would argue for incorporating constructs to test how protection success influences different organizational (alliance) outcomes, as well as how organizational (alliance) outcomes influence protection behaviour or success.

4.2.3 Mixed method approaches. The remaining five papers used a mix of quantitative and qualitative methods. The authors found three papers combining quantitative questionnaires with qualitative interviews. Norman (2001) and Howells *et al.* (2003) used mixed methods to either complement and triangulate the results of individual approaches or to mitigate the commonly used method bias (Podsakoff *et al.*, 2003).

Summing up, the authors did not find any literature review paper on knowledge protection undertaken so far. The high occurrence of analytic discussions, explorative research and case studies is an indication that research on knowledge protection is still in its early stages.

4.3 Role of the IT artefact

This literature review reveals that the role of the IT artefact is rather neglected in research concerned with the topic of knowledge protection. Using the five views from Orlikowski and Iacono (2001), the authors analyzed the papers in the set according to the tool, ensemble, nominal, computational and proxy views.

One paper (Zhou and Liu, 2010) belongs to the computational view which is concerned with the computational power of IT (algorithms, models) as separated from the organizational context and from the interaction with the people using it (Orlikowski and Iacono, 2001); their paper reports on the features of the protection tool (Zhou and Liu, 2010).

Eight papers can be allocated to the nominal view. This considers the IT artefact as absent, i.e. as an omitted variable which, although used incidentally or as background information, the conceptual and analytical analyses lie elsewhere. Papers here discuss the influence on the application of IT (Bloodgood and Salisbury, 2001), consider IT as an influencing factor of knowledge security success (Neville *et al.*, 2003), or focus in their analysis on IPR effectiveness to protect IT innovations (Arundel, 2001; Kale *et al.*, 2000). The latter could be the basis for following up research from a tool perspective, i.e. by investigating the relationship between IT and knowledge protection.

One paper belongs to the ensemble view. The ensemble view considers how IT emerged in contextual settings as inseparable from its use by people, i.e. how the use of social media leads to various challenges for knowledge protection (Väyrynen *et al.*, 2013).

The tool view considers the IT artefact as an independent variable ("black box") influencing certain constructs such as protection behaviour or success. Two papers investigate the IT artefact as a productivity tool (cf. Orlikowski and Iacono, 2001) focussing on how IT, like security communication languages or role-based access control, helps to increase the knowledge protection capabilities of organizations (Upadhyaya *et al.*, 2011).

The proxy view focusses on how IT is perceived by individuals, how it is spread within organizations (diffusion patterns) or how it discusses the value of IT as a resource or investment of organizations. On this view, the authors did not find any papers either.

Our general impression is that the literature on knowledge protection mostly fails to consider the IT artefact, as it originates in the research field of strategic management. This, again, shows that research on supportive IT for knowledge protection is under-researched, with the primary focus still being on understanding its basic principles. Support in general and IT support in particular seem promising avenues for further research. Based on the work of Zhou and Liu (2010), for example, one could investigate IT as a means for enhancing knowledge protection, and explore how such an IT artefact could influence protection success. Or one could investigate IT as an influencing factor challenging knowledge protection quantitatively. Here, Väyrynen *et al.*'s (2013) explorative approach towards overcoming challenges of social media for knowledge protection could inspire follow-up research. Future studies should investigate the development and introduction of IT as supporting knowledge protection in different organizational settings.

4.4 Theoretical perspectives

Our review found that the literature on knowledge protection is in the main concerned with the tension arising between knowledge sharing and protection (Jordan and Lowe, 2004). Inter-organizational collaborations exist to learn from each other (Kale *et al.*, 2000); however, they are often characterized by inequalities and asymmetries (Hamel, 1991). The assumption that it is rational for an organization to absorb more knowledge than it is prepared to share, rather creates sub-optimal outcomes for the collaboration as a whole (Jordan and Lowe, 2004). This so-called "learning paradox" is accompanied by the "boundary paradox": organizations need to be open to information flows from external sources while they need to protect their internal knowledge (Quintas *et al.*, 1997; Norman, 2002; Jordan and Lowe, 2004; Lee *et al.*, 2007). The authors found that different theoretical lenses were used to investigate the issue of protecting internal and absorbing external knowledge.

The authors investigated the theoretical and conceptual views explicitly stated in the papers and share the view of Jordan and Lowe (2004) that there are basically three theoretical lenses through which knowledge protection has been discussed so far:

1. The transaction cost perspective.
2. The relational perspective.
3. The resource-based perspective.

However, the distinctions (Jordan and Lowe, 2004) are not always easy to make. After providing an overview of the different theory streams, the authors also indicate how each stream contributes to research by adopting the taxonomy proposed by Gregor (2006).

4.4.1 Transaction cost economics. Transaction cost economics (TCE) try to explain alliance formations as a means to reducing production and transaction costs (Williamson, 1985; Kale *et al.*, 2000). The first major stream focusses on extending TCE to the notion of knowledge. Liebeskind (1996) argued that firms can only create and sustain competitive advantage when they are able to protect valuable knowledge and if they have particular institutional capabilities to protect knowledge more effectively than through market contracting. From a protection point of view, it is further argued that firms should preferably use equity-based partnerships (Liebeskind, 1996), and that a transaction's potential to protect knowledge might influence governance decisions (Mayer (2006). TCE seems to be a valuable approach to providing answers to and receive contributions from knowledge protection, as the right selection of alliance forms (Oxley, 1999; Li *et al.*, 2008) and governance structures (Li *et al.*, 2008) can mitigate the risks. However, the existing body of literature primarily focusses on the formal and the legal dimension of knowledge protection, while neglecting the tacit dimension.

The scholarly contributions to knowledge protection from a TCE perspective are in the main descriptive rather than prescriptive, as the stated aim often is to "identify determinants of alliance structures rather than to offer advice to managers on alliance design *per se*" (Jordan and Lowe, 2004).

4.4.2 Resource-based view. To sustain their competitive advantage, firms need resources and capabilities (specific combinations of resources), and they have to develop a business strategy that makes use of these resources and capabilities (Grant, 1991). Assuming knowledge-based resources are the most important source of competitive advantage (Kogut and Zander, 1992; DeSouza, 2006), the knowledge protection literature discusses knowledge protection as a firm's capability (Gold *et al.*, 2001), as well as a firm's set of measures (Baughn *et al.*, 1997) or influencing factors (Norman, 2002) to hinder other external organizations to absorb a firm's knowledge. For knowledge protection, a firm needs both knowledge infrastructure capability and knowledge process capability. Knowledge protection is a part of the latter and hence it is vital to generate new knowledge and competitive advantage. For a firm's set of measures, theories like absorptive capacity, organizational learning and knowledge sharing are of importance (Jordan and Lowe, 2004), especially with respect to explaining the boundary paradox.

The authors found normative guidance in both perspectives, e.g. papers providing a model recommending protection as a capability (Gold *et al.*, 2001), as a framework to balance sharing and protecting (Baughn *et al.*, 1997) and also in a predictive way (Urcuyo and Kunnathur, 2002).

4.4.3 Relational perspective. This perspective mainly focusses on how relational capital, i.e. mutual trust, respect and friendship in inter-organizational relationships influence the learning paradox (Kale *et al.*, 2000; Jordan and Lowe, 2004). In literature, it is pointed out that firms' relationships in alliances need to gain more attention, as they play a big role in solving the boundary paradox (Kale *et al.*, 2000). Further, the characteristics of knowledge and those of partners need to be considered, as well as specific mechanisms for protection (Norman, 2002). On the one hand, higher trust leads to a lower protection level between alliance members (Norman, 2004), and, on the other hand, formal governance indicates a lack of trust and is only adopted when relational capital is lacking (Li *et al.*, 2008).

From this perspective, the authors found only literature making statements on testing, explaining and predicting, e.g. the greater the extent of knowledge protection, the greater the relational capital will be (Lee *et al.*, 2007), or trust between alliance members and their level of knowledge protection (Norman, 2002).

Summing up, the vast majority of papers failed to present their insights in a specific theoretical framework. This shows that knowledge protection is still in its infancy. Moreover, the potential of theories that are traditionally used to inform the management of information security, like control theory (Hedström *et al.*, 2011), has not been sufficiently exploited for knowledge protection. In contrast to Jordan and Lowe (2004), the authors found that there are not always clear distinctions between the perspectives and there was little evidence that the relational perspective constitutes a particular knowledge protection stream – the relational perspective of knowledge protection being in any case widely unexplored.

However, the authors would encourage further work on this field. With respect to research results, the authors did not find any papers that develop and evaluate system designs or offer prescriptive design guidelines, as proposed by design science research (Hevner *et al.*, 2004).

4.5 Measures

Knowledge protection measures are discussed from many different angles in pertinent literature. The authors consider measures as any efforts of organizations to protect knowledge at:

- the risk management layer;
- the knowledge protection objectives layer; and
- the knowledge protection mechanisms layer.

The risk management and knowledge protection objectives layers focus on the formulation of abstract goals and strategies to mitigate risks, while the knowledge protection mechanisms layer focusses on the enforcement of the strategies and goals. The authors aggregate these views in a more holistic perspective (Figure 2). The goal is to structure the discussion on knowledge protection measures and the identification of research gaps.

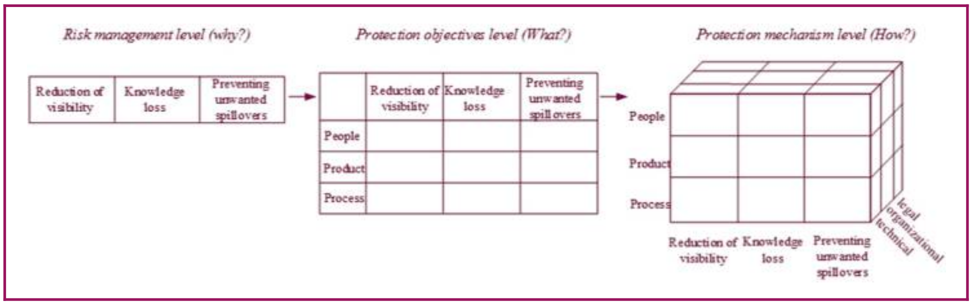
To determine which measures are suitable for their knowledge protection, organizations have to set their own goals and requirements. One of the key questions they should ask themselves is *why* should we protect knowledge? These high-level knowledge protection goals are part of organizational risk management strategy and hence should be integrated accordingly. The literature revealed three dominant motives for knowledge protection:

1. the reduction of knowledge visibility;
2. the reduction of knowledge loss, e.g. through employee retention; and
3. the reduction of undesired knowledge spillovers and leakages.

On this level, the literature discusses knowledge risk mitigation frameworks, identifying knowledge risk categories and proposing mitigation approaches (Trkman and DeSouza, 2012; Aljafari and Sarnikar, 2009; Boyles *et al.*, 2009), especially arising from the use of social media (Väyrynen *et al.*, 2013), or present protection frameworks that help firms to develop mechanisms and policies to protect knowledge (Randeree, 2006). Further, propositions for using different types of knowledge structures to balance sharing and protecting (Lucas, 2010).

The next level refers to *what* knowledge organizations should protect. Based on the COBIT recommendations for control frameworks (ISACA, 2012), the knowledge protection goals are broken down into more concrete objectives. Such objectives define the goal of implementing measures and are designed to provide reasonable assurance that risk management goals are achieved and undesired events prevented. In this literature set, there are basically three categories of control objectives, i.e. people, products and

Figure 2 Levels of knowledge protection


Risk management level (why?)
Reduction of visibility
Knowledge loss
Preventing unwanted spillovers
Protection objectives level (What?)
Reduction of visibility
Knowledge loss
Preventing unwanted spill overs
People
Product
Process
Protection mechanism level (How?)
People
Product
Process
Reduction of visibility
Knowledge loss
Preventing unwanted spillovers
legal
organizational
technical

processes (DeSouza and Vanapalli, 2005; DeSouza, 2006). Each dimension in the risk management layer may refer to a specific knowledge protection objective. The product dimension deals with explicit knowledge, the process dimension with protecting knowledge generation and application and the people dimension with tacit knowledge.

Based on the COBIT recommendations for control frameworks (ISACA, 2012), control objectives need to be enforced by concrete mechanisms, i.e. configurations, practices, procedures or organizational structures. Here the question that needs to be posed is: *How can this enforcement be realized?* Mechanisms for knowledge protection have been described by different scholars (Olander *et al.*, 2011; Trkman and DeSouza, 2012; de Faria and Sofka, 2010; Harabi, 1995; Howells *et al.*, 2003; Kale *et al.*, 2000). The authors noticed three main types discussed in the literature:

1. Legal (Hertzfeld *et al.*, 2006).
2. Organizational (Norman, 2001).
3. Technical (Bertino *et al.*, 2006).

Especially organizations offering knowledge-intensive services typically implement a mix of different formal and informal mechanisms (Amara *et al.*, 2008; Miles *et al.*, 2000). Table II gives an overview of the mechanisms found in the literature.

The protection of knowledge held by **people** mainly focusses on tacit knowledge. In *Organizational mechanisms*, recruiting and indoctrination is used to employ and hire people meeting knowledge protection requirements (DeSouza and Vanapalli, 2005; Olander *et al.*, 2011). Monitoring of employees by means of counterintelligence teams can be used to proactively identify potential leaks, as successfully applied in the defence and intelligence sector (DeSouza and Vanapalli, 2005). Education and training (DeSouza and Vanapalli, 2005) serve to improve employees' awareness of protection responsibilities (Olander *et al.*, 2011; Baughn *et al.*, 1997). The implementation of security clearances has been mentioned to identify what knowledge is pertinent to a specific role (DeSouza and Vanapalli, 2005). Leadership focusses on ensuring sufficient resources to implement measures, and it should identify core protection capabilities. Finally, in partnership with external organizations, measures like establishing dedicated roles for consulting/advising in unclear or vague situations can be established (Norman, 2001). *Legal measures* to protect tacit knowledge refer to contract clauses like non-disclosure agreements (Olander *et al.*, 2011; Hannah, 2005; Norman, 2001), non-competition agreements (Cohen *et al.*, 2000; Hertzfeld *et al.*, 2006) or ground rules contracts (Olander *et al.*, 2011) which serve to provide a safe basis for collaboration (Olander *et al.*, 2011). No technical measures for protecting tacit knowledge could be found, which suggests that this could be a promising avenue for future research.

Table II Portfolio of knowledge protection measures

Type of measure\Dimension	*People*	*Product*	*Process*
Organizational	Recruiting and Indoctrination Counterintelligence Awareness training Education Leadership Role creation	Awareness training Lead time Secrecy/concealment Standardization/Annotation	Awareness training Leadership Accountability and separation of duties
Legal	NDAs NCAs Ground rules	NDAs NCAs Ground rules IPR	NDAs NCAs IPR Ground rules Accountability and separation of duties
Technical	–	Securing devices Standardization/Annotation	(physical) access control Securing comm. channels Securing devices

The second dimension is the protection of knowledge as a **product**, i.e. an object or artefact, i.e. knowledge reposited in documents, which is subject to common security procedures (DeSouza and Vanapalli, 2005). Amongst *organizational mechanisms*, lead time advantages towards competitors (Li *et al.*, 2008; Olander *et al.*, 2011; Monteiro *et al.*, 2011, Howells *et al.*, 2003) can be a suitable mechanism for organizations who are the first to enter the market (Hurmelinna-Laukkanen and Puumalainen, 2007). In this way, organizations can prevent unwanted appropriation of knowledge that would enable others to enter the market too soon after their own presence. Practical concealment/secrecy describes the physical restriction of a certain group of people from knowledge (Olander *et al.*, 2011; Hurmelinna-Laukkanen and Puumalainen, 2007). Finally, awareness training also serves to protect knowledge. *Legal mechanisms* refer to all kinds of IPR and are essentially the same mechanisms as those for the people dimension. IPR include the following measures: patents, trade secrets, copyrights and trademarks (Hannah, 2005; Hertzfeld *et al.*, 2006; Harabi, 1995). Apart from being costly, IPR however has other drawbacks, including that a great many innovations fall outside of its protection (Liebeskind, 1997), that many nations do not provide enough legal protection (Snyder and Crescenzi, 2009) and critical knowledge first has to be made public, such as for patenting, for example (Hannah, 2005). Especially organizations offering knowledge-intensive services face more challenges when using patents than manufacturing firms (Amara *et al.*, 2008). Patents are, in fact, considered to be rather ineffective for the purpose of protecting innovations (Harabi, 1995) when imitation is costly and first-mover advantages are important (Encaoua *et al.*, 2006), which makes them rather unattractive, at least for service companies (Howells *et al.*, 2003). Trade secrets do not hinder rivals from acting opportunistically as third parties cannot be prosecuted for obtaining critical knowledge from organizations unaware of spillovers (Liebeskind, 1997). Copyrights provide organizations with a replication monopoly but actually do not protect knowledge (Liebeskind, 1997). Trademarks serve to protect distinctive names or observable symbols that belong to an organization. Despite all these limitations, it seems that IPR is currently the most accepted and widespread approach to knowledge protection (Hertzfeld *et al.*, 2006; Hannah, 2005). Additionally, contractual measures also serve to protect explicit knowledge, as they often address knowledge that is not to be shared (Norman, 2001). Overall, legal protection measures for the product dimension are more widespread (Hertzfeld *et al.*, 2006) and mainly come from the IPR perspective. In *Technical measures*, standardization of documentation processes, tagging and segmentation of knowledge documents is important to:

- enable quicker search, retrieval and comprehension of best practices for protection;
- track documents containing knowledge, as well as their movement and utilization; and
- guarantee access only to corresponding clearances (DeSouza and Vanapalli, 2005).

Further, securing devices offers another form of knowledge protection, particularly mobile devices (DeSouza and Vanapalli, 2005).

The third dimension is the protection of knowledge about or embodied in organizational **processes** (DeSouza and Vanapalli, 2005; Norman, 2001), e.g. technical expertise or strategic knowledge (Norman, 2001). First, *organizational* protection can be implemented through awareness training (Baughn *et al.*, 1997), the establishment of organizational roles such as a gatekeeper or communication stars appointed to monitor information flows (Norman, 2001), leadership (DeSouza and Vanapalli, 2005) or determining accountability and separation of duties (DeSouza and Vanapalli, 2005). Further, securing knowledge channels and devices by means of authorization procedures (DeSouza and Vanapalli, 2005) is a further measure. In *Legal mechanisms*, again, contractual measures, as well as IPR, also serve to protect this type of knowledge. *Technical mechanisms* like access control can be enforced by authentication implemented through identification badges, biometric sensors, voice recognition or traditional passwords.

It became apparent that research on protecting knowledge is scattered and focusses on specific aspects. To the best of the authors' knowledge, no overview of measures could be found. Here, the authors consider this paper as a starting point which should guide future research. Interestingly, none of the investigated papers paid any attention to the links between the *why*, the *what* and the *how* dimensions. Although both the literature and practice have highlighted the need for aligning the top-level management perspective with concrete measures (Ahmad *et al.*, 2014) as well the need for an overall strategy (Alstete, 2003; Olander *et al.*, 2011), this topic is neglected in the current scholarly literature. However, scientific work on factors influencing the effectiveness of knowledge protection, e.g. governance structure (Oxley, 1999), knowledge capabilities (Gold *et al.*, 2001), trust (Norman, 2004), scope between partners, their learning intent (Norman, 2004) or employees' perceptions (Hannah, 2005), provides a promising basis for the investigation of these links. Due to the increasingly growing number of digital communication channels, the need for technical measures will also increase. As the authors found only few technical measures and especially none for tacit knowledge, it seems that this suggests another promising avenue for future research.

Summing up, the authors discussed 48 papers on knowledge protection from various angles and identified several shortcomings in the literature. First, there is a lack of in-depth investigations which are necessary to provide more than high-level protection measures in a generalized way. Second, the IT artefact is widely neglected, especially for the protection of tacit knowledge. Third, the major part of the literature lacks references to specified theoretical frameworks and, hence, misses the opportunity to make theoretical contributions. Fourth, the tacit dimension of knowledge protection is widely neglected. Most papers strongly focus on formal and informal measures which protect explicit knowledge. Finally, the literature widely fails to provide firms with holistic protection strategies, although the need has been raised, and focusses instead on the application of specific measures. In the following, a research agenda addressing these shortcomings is proposed.

5. A future research agenda

Within the literature review, the authors investigated the research on knowledge protection. Based on these results, promising research directions for future research can be discussed.

5.1 Opening the black box around the protection of tacit knowledge

The authors found that research mainly focusses on formal organizational collaborations, and was concentrated on alliances in the automotive sector. Informal collaborations between organizations, such as communities of practice, received little attention so far. This is surprising as most organizations are engaged in informal collaborations far more than in formal collaborations, including those involving suppliers or customers, for example. The higher penetration of social media further increases the number of informal networks, of course, so this aspect gains even higher relevance (Väyrynen *et al.*, 2013). Hence, the authors recommend that future research on knowledge protection should take into account informal collaborations and particularly social networks.

Formal and explicit knowledge emerged as the primary focus in the majority of papers. Particularly, the perspective of IPR using patents or trade secrets was investigated. Unclassified documented knowledge or even tacit knowledge was underrepresented by far. In light of the fact that much organizational knowledge, and especially crucial knowledge, is tacit (Alavi and Leidner, 2001), researchers should pay more attention to the protection of tacit knowledge, which brings into play the paradox of knowledge visibility. On the one hand, organizations should increase the visibility of knowledge to facilitate the KM. On the other, greater transparency also enhances the risk of unwanted spillovers which challenges knowledge protection. The investigation of this trade-off provides another avenue for future research.

5.2 Analysing the phenomena in-depth

The authors found a fair number of conceptual papers, case studies and broad explorative empirical work in this literature review. The lack of empirical validation, however, restricts the value of the recommendations these conceptual papers can make. Especially case studies and explorative papers investigate knowledge protection phenomena on abstract levels. Using the results to inform the design of supportive measures, and particularly, supportive IT, seems challenging due to the fact that the effectiveness of knowledge protection depends on the individual company and its situational aspects (Ford and Staples, 2010) which are rarely considered so far. Consequently, there is a need to perform more empirical work such as observations and ethnography to gain more in-depth understanding of knowledge protection phenomena (Pawlowski *et al.*, 2014). Maier and Thalmann (2012) propose a procedure for the application of ethnographies to the in-depth investigation of phenomena of knowledge work which, at the same time, aim to design supportive IT. This justifies the authors in proposing a shift of focus from the organizational or alliance level down to the level of individuals who are responsible for knowledge leakage. Such individual-centric studies would particularly benefit from in-depth studies.

5.3 Designing supportive IT

Tool support and particular IT support is crucial for the application of knowledge protection in organizations (von Krogh, 2012). However, research on IT artefacts is currently underdeveloped, especially the tool view. The authors propose to apply more design science research (Hevner *et al.*, 2004) in the domain of knowledge protection and to develop and evaluate supportive IT. Here, the particular challenge is to focus not only on documented and classified knowledge but also on IT aimed at enhancing employees' awareness. Research in this direction is needed to offer possibilities to apply knowledge protection measures and to increase the application of knowledge protection in organizations. From the authors' perspective, these IT artefacts should provide guidance and decision support rather than restrict behaviour. Especially in light of the predominantly tacit nature of knowledge and the unstructured manner of knowledge work (Maier, 2007), such simple restrictions do not seem appropriate.

5.4 Viewing knowledge protection through a theoretical lens

A fourth future research direction argues for the need to take greater account of theoretical frameworks for the investigation of knowledge protection phenomena. The lack of theoretical references dominates this review, and while it shows that, on the one hand, knowledge protection research is still in its infancy, it probably also indicates the need to develop theories on knowledge protection. Hence, the authors recommend the usage of theories in general and particularly from the field of KM and information security.

5.5 Managing the portfolio of knowledge protection measures more systematically

During the literature review, the authors identified a set of knowledge protection measures on three different levels. But, as it turns out, the usage of these measures is currently not aligned to a knowledge protection strategy. Even as some scholars argue for the need of such a strategy, little research into this aspect could be found. From the authors' point of view, any knowledge protection strategy should always be linked to an organization's information security strategy, both of which form an integral part of risk management. Research on how to adapt well-established procedures from information security to knowledge protection would therefore seem valuable.

6. Summary

To the best of the authors' knowledge, this paper is the first comprehensive literature review undertaken on knowledge protection. It shows that, despite its central importance to organizational competitiveness (Liebeskind, 1996), knowledge protection is an under-researched topic in KM. The authors analyzed 48 papers, and the key results are summarized according to the five analytical dimensions in Table III.

The authors found that research on knowledge protection widely ignores informal collaborations, such as communities of practice, while tending to focus on contract- or equity-based collaborations. Related to this, the main focus in the current literature is on the protection of explicit knowledge, while the tacit knowledge dimension is, by and large, neglected. Furthermore, IT artefacts to protect knowledge, e.g. decision-support systems, are rarely proposed. Additionally, most of the investigated papers are conceptual and do not investigate knowledge protection from the perspective of a specific theory. Based on these findings, the authors identified promising avenues for further research and proposed a research agenda. Future research should deal with the protection of tacit knowledge, more in-depth empirical investigations, a stronger focus on IT support and a stronger consideration of theories in knowledge protection research, as well as research on how organizations could develop their own strategy of knowledge protection.

This research has some limitations. First, the review was restricted to those journals which the authors could access, and to those that were indexed by the search hosts, thereby inevitably excluding some journals. Second, other dimensions of analysis could be adopted, but the authors of this review considered that the ones they adopted here – research domains, methods and models, the role of the IT artefacts, theoretical perspectives, as well as measures revealed the most interesting insights for future research. These two limitations imply that the authors cannot claim that this review is exhaustive, and hence, they are merely proposing *a* research agenda and not *the* research agenda (cf. Seidel *et al.*, 2010). However, the authors believe that research in the proposed directions would substantially contribute to the body of scholarly knowledge on knowledge protection and help to put the topic on the map in the KM domain.

Table III Implications for academia and practice

Analytical dimension	*Implications for academia*	*Implications for practice*
Research domain	Tacit knowledge, as well as informal alliances or (social) networks, is under researched so far. However, they provide promising research opportunities and should be taken into account	Knowledge protection should focus on the prevention of knowledge loss, the reduction of knowledge spillovers and the prevention of knowledge leakage
Research models	Knowledge protection phenomena need to be investigated in depth to test the assumptions stated in many conceptual papers. This could be supported through case studies which test models and concepts in organizational settings	Few knowledge protection, concepts and blueprints are empirically tested. Hence, existing models and their recommendations should be handled with care
Role of IT artefact	Due to the mostly conceptual nature of knowledge protection research, the IT tool perspective is widely neglected so far. However, for testing proposed models and behavioural relationships, IT artefacts should be developed and evaluated by applying a design science research procedure	While the review identified the need for IT-supporting knowledge protection, IT tool support was not. The development of IT tools seems, however, to offer a promising business opportunity and could improve knowledge protection measures
Theoretical perspectives	Knowledge protection research would greatly benefit from being more theory-based, with information security theories and KM theories appearing to be particularly promising avenues	The adoption of models and guidelines from the domain of information security and compliance seems promising for establishing organizational knowledge protection
Measures	There is little research on specific knowledge protection measures and particularly technical measures which can be automatically enforced. A need emerges here for research on how to adapt well-established procedures from information security to enforce and audit knowledge protection, as well as an overarching framework or strategy for knowledge protection	Knowledge protection measures need to be coordinated and aligned to organizational risk management Knowledge protection measures should be defined and enforced for each knowledge protection goal

References

Ahmad, A., Bosua, R. and Scheepers, R. (2014), “Protecting organizational competitive advantage: a knowledge leakage perspective”, *Computers & Security*, Vol. 42, pp. 27-39.

Alavi, M. and Leidner, D.E. (2001), “Review: knowledge management and knowledge management systems: conceptual foundations and research issues”, *MISQ*, Vol. 25 No. 1, pp. 107-136.

Aljafari, R. and Sarnikar, S. (2009), “A framework for assessing knowledge sharing risks in interorganizational networks”, *AMCIS 2009 Proceedings*, *San Francisco, CA*.

Alstete, J. (2003), “Trends in corporate knowledge asset protection”, *Journal of Knowledge Management Practice*, Vol. 4.

Amara, N., Landry, R. and Traoré, N. (2008), “Managing the protection of innovations in knowledge-intensive business services”, *Research Policy*, Vol. 37 No. 9, pp. 1530-1547.

Arundel, A. (2001), “The relative effectiveness of patents and secrecy for appropriation”, *Research policy*, Vol. 30 No. 4, pp. 611-624.

Asllani, A. and Luthans, F. (2003), “What knowledge managers really do: an empirical and comparative analysis”, *Journal of Knowledge Management*, Vol. 7 No. 3, pp. 53-66.

Bachlechner, D., Thalmann, S. and Manhart, M. (2014), “Auditing service providers: supporting auditors in cross-organizational settings”, *Managerial Auditing Journal*, Vol. 29 No. 4, pp. 286-303.

Baughn, C.C., Denekamp, J.G., Stevens, J.H. and Osborn, R.N. (1997), “Protecting intellectual capital in international alliances”, *Journal of World Business*, Vol. 32 No. 2, pp. 103-117.

Bertino, E., Khan, L.R. and Sandhu, R. (2006), “Secure knowledge management: confidentiality, trust, and privacy”, *IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans*, Vol. 36 No. 3, pp. 429-438.

Bloodgood, J.M. and Salisbury, W.D. (2001), “Understanding the influence of organizational change strategies on information technology and knowledge management strategies”, *Decision Support Systems*, Vol. 31 No. 1, pp. 55-69.

Boyles, J.E., Kirschnick, F., Kosilov, A., Yanev, Y. and Mazour, T. (2009), “Risk management of knowledge loss in nuclear industry organisations”, *International Journal of Nuclear Knowledge Management*, Vol. 3 No. 2, pp. 125-136.

Brouwer, E. and Kleinknecht, A. (1999), “Innovative output, and a firm’s propensity to patent: an exploration of CIS micro data”, *Research Policy*, Vol. 28 No. 6, pp. 615-624.

Bruck, P.A., Motiwalla, L. and Foerster, F. (2012), “Mobile learning with micro-content: a framework and evaluation”, *Proceedings of the 25th Bled eConference*, *Bled*.

Chan, P.C.W. and Lee, W.B. (2011), “Knowledge audit with intellectual capital in the quality management process: an empirical study in an electronics company”, *The Electronic Journal of Knowledge Management*, Vol. 9 No. 2, pp. 98-116.

Cheung, C., Ma, R., Wong, W. and Tse, Y. (2012), “Development of an organizational knowledge capabilities assessment (OKCA) method for innovative technology enterprises”, *World Academy of Science, Engineering and Technology*, No. 67, pp. 54-65.

Cohen, W.M., Nelson, R.R. and Walsh, J.P. (2000), “Protecting their intellectual assets: appropriability conditions and why US manufacturing firms patent (or not)”, NBER Working Paper No. 7552, National Bureau of Economic Research.

de Faria, P. and Sofka, W. (2010), “Knowledge protection strategies of multinational firms – a cross-country comparison”, *Research Policy*, Vol. 39 No. 7, pp. 956-968.

Delone, W.H. and McLean, E.R. (1992), “Information systems success: the quest for the dependent variable”, *Information Systems Research*, Vol. 3 No. 1, pp. 60-95.

DeSouza, K.C. (2006), “Knowledge security: an interesting research space”, *Journal of Information Science and Technology*, Vol. 3 No. 1, pp. 1-7.

DeSouza, K.C. and Vanapalli, G.K. (2005), “Securing knowledge in organizations: lessons from the defense and intelligence sectors”, *International Journal of Information Management*, Vol. 25, pp. 85-98.

Dhillon, G. and Torkzadeh, G. (2006), “Value-focused assessment of information system security in organizations”, *Information Systems Journal*, Vol. 16 No. 3, pp. 293-314.

Ding, X.-H. and Huang, R.-H. (2010), "Effects of knowledge spillover on inter-organizational resource sharing decision in collaborative knowledge creation", *European Journal of Operational Research*, Vol. 201 No. 3, pp. 949-959.

Encaoua, D., Guellec, D. and Martinez, C. (2006), "Patent systems for encouraging innovation: lessons from economic analysis", *Research Policy*, Vol. 35 No. 9, pp. 1423-1440.

Ford, D.P. and Staples, S. (2010), "Are full and partial knowledge sharing the same?", *Journal of Knowledge Management*, Vol. 14 No. 3, pp. 394-409.

Gerber, M. and von Solms, R. (2001), "From risk analysis to security requirements", *Computers & Security*, Vol. 20 No. 7, pp. 577-584.

Gerber, M. and von Solms, R. (2005), "Management of risk in the information age", *Computers & Security*, Vol. 24 No. 1, pp. 16-30.

Gold, A.H., Malhotra, A. and Segars, A.H. (2001), "Knowledge management: an organizational capabilities perspective", *Journal of Management Information Systems*, Vol. 18 No. 1, pp. 185-214.

Grant, R.M. (1991), "The resource-based theory of competitive advantage: implications for strategy formulation", *Knowledge and Strategy*, Vol. 33 No. 3, pp. 3-23.

Gregor, S. (2006), "The nature of theory in information systems", *MISQ*, Vol. 30 No. 3, pp. 611-642.

Hamel, G. (1991), "Competition for competence and interpartner learning within international strategic alliances", *Strategic Management Journal*, Vol. 12 No. S1, pp. 83-103.

Hannah, D.R. (2005), "Should I keep a secret? The effects of trade secret protection procedures on employees' obligations to protect trade secrets", *Organization Science*, Vol. 16 No. 1, pp. 71-84.

Harabi, N. (1995), "Appropriability of technical innovations an empirical analysis", *Research policy*, Vol. 24 No. 6, pp. 981-992.

Hedström, K., Kolkowska, E., Karlsson, F. and Allen, J.P. (2011), "Value conflicts for information security management", *The Journal of Strategic Information Systems*, Vol. 20 No. 4, pp. 373-384.

Hertzfeld, H.R., Link, A.N. and Vonortas, N.S. (2006), "Intellectual property protection mechanisms in research partnerships", *Research Policy*, Vol. 35 No. 6, pp. 825-838.

Hevner, A.R., March, S.T., Park, J. and Ram, S. (2004), "Design science in information systems research", *MISQ*, Vol. 28 No. 1, pp. 75-105.

Howells, J., Blind, K., Elder, J. and Evangelista, R. (2003), "Knowledge regimes, appropriability and intellectual property protection: a conceptual framework for services", in Lind, K., Elder, J., Schmoch, U., Anderson, B., Howells, J., Miles, I., Roberts, J., Green, L., Evangilista, R., Hipp, C. and Herstatt, C. (Eds), *Patents in the Service Industries*, Fraunhofer Institute Systems and Innovation Research.

Hurmelinna-Laukkanen, P. and Puumalainen, K. (2007), "Nature and dynamics of appropriability: strategies for appropriating returns on innovation", *R&D Management*, Vol. 37 No. 2, pp. 95-112.

Ilvonen, I. (2013), "Knowledge security-a conceptual analysis", *PhD thesis*, Tampere University of Technology, Tampere.

ISACA (2012), *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*, ISACA.

Jennex, M. (2009), "Assessing knowledge loss risk", *Americas Conference on Information Systems*, San Francisco, CA.

Jennex, M. and Durcikova, A. (2013), "Assessing knowledge loss risk", *2013 46th Hawaii International Conference on System Sciences (HICSS*), Wailea, HI, pp. 3478-3487.

Jennex, M. and Olfman, L. (2005), "Assessing knowledge management success", *International Journal of Knowledge Management*, Vol. 1 No. 2, pp. 33-49.

Jennex, M. and Zyngier, S. (2007), "Security as a contributor to knowledge management success", *Information Systems Frontiers*, Vol. 9 No. 5, pp. 493-504.

Jordan, J. and Lowe, J. (2004), "Protecting strategic knowledge: insights from collaborative agreements in the aerospace sector", *Technology Analysis & Strategic Management*, Vol. 16 No. 2, pp. 241-259.

Kale, P., Singh, H. and Perlmutter, H. (2000), “Learning and protection of proprietary assets in strategic alliances: building relational capital”, *Strategic Management Journal*, Vol. 21, pp. 217-237.

Khamseh, H.M. and Jolly, D.R. (2008), “Knowledge transfer in alliances: determinant factors”, *Journal of Knowledge Management*, Vol. 12 No. 1, pp. 37-50.

Kogut, B. and Zander, U. (1992), “Knowledge of the firm, combinative capabilities, and the replication of technology”, *Organization Science*, Vol. 3 No. 3, pp. 383-397.

Lee, C.C. and Yang, J. (2000), “Knowledge value chain”, *Journal of Management Development*, Vol. 19 No. 9, pp. 783-794.

Lee, S.C., Chang, S.N., Liu, C.Y. and Yang, J. (2007), “The effect of knowledge protection, knowledge ambiguity, and relational capital on alliance performance”, *Knowledge and Process Management*, Vol. 14 No. 1, pp. 58-69.

Li, D., Eden, L., Hitt, M.A. and Ireland, R.D. (2008), “Friends, acquaintances, or strangers? Partner selection in R&D alliances”, *Academy of Management Journal*, Vol. 51 No. 2, pp. 315-334.

Liebeskind, J.P. (1996), “Knowledge, strategy and the theory of the firm”, *Strategic Management Journal*, Vol. 17 No. Winter Special Issue, pp. 93-107.

Liebeskind, J.P. (1997), “Keeping organizational secrets: protective institutional mechanisms and their costs”, *Industrial and Corporate Change*, Vol. 6 No. 3, pp. 623-663.

Link, A.N. and Ruhm, C.J. (2011), “Public knowledge, private knowledge: the intellectual capital of entrepreneurs”, *Small Business Economics*, Vol. 36 No. 1, pp. 1-14.

Lucas, L.M. (2010), “The evolution of organizations and the development of appropriate knowledge structures”, *Journal of Knowledge Management*, Vol. 14 No. 2, pp. 190-201.

Maier, R. (2007), *Knowledge Management Systems: Information and Communication Technologies for Knowledge Management*, 3rd ed., Springer, Berlin.

Maier, R., Hädrich, T. and Peinl, R. (2009), *Enterprise Knowledge Infrastructures*, 2nd ed., Springer, Berlin.

Maier, R. and Thalmann, S. (2012), “Collaborative ethnography for information systems research studying knowledge work practices and designing supportive information systems”, *Australasian Journal of Information Systems*, Vol. 17 No. 2, pp. 137-160.

Mayer, K.J. (2006), “Spillovers and governance: an analysis of knowledge and reputational spillovers in information technology”, *Academy of Management Journal*, Vol. 49 No. 1, pp. 69-84.

Miles, I., Andersen, B., Boden, M. and Howells, J. (2000), “Service production and intellectual property”, *International Journal of Technology Management*, Vol. 20 No. 1, pp. 95-115.

Monteiro, F., Mol, M.J. and Birkinshaw, J. (2011), “External knowledge access versus internal knowledge protection: a necessary trade-off?”, *Academy of Management Proceedings, Academy of Management*, No. 1, pp. 1-6.

Nelson, R.R. and Winter, S.G. (1982), *An Evolutionary Theory of Economic Change*, Harvard University Press, Cambridge.

Neville, K., Powell, P. and Panteli, N. (2003), “Knowledge and security”, *AMCIS 2003 Proceedings, Tampa, Florida*.

Nonaka, I. (1994), “A dynamic theory of organizational knowledge creation”, *Organization Science*, Vol. 5 No. 1, pp. 14-37.

Nonaka, I. and Takeuchi, H. (1995), *The Knowledge-Creating Company*, Oxford University Press, New York, NY.

Norman, P.M. (2001), “Are your secrets safe? Knowledge protection in strategic alliances”, *Business Horizons*, Vol. 44 No. 6, pp. 51-60.

Norman, P.M. (2002), “Protecting knowledge in strategic alliances: resource and relational characteristics”, *The Journal of High Technology Management Research*, Vol. 13 No. 2, pp. 177-202.

Norman, P.M. (2004), “Knowledge acquisition, knowledge loss, and satisfaction in high technology alliances”, *Journal of Business Research*, Vol. 57 No. 6, pp. 610-619.

Olander, H., Hurmelinna-Laukkanen, P. and Heilmann, P. (2011), "Do SMEs benefit from HRM-related knowledge protection in innovation management?", *International Journal of Innovation Management*, Vol. 15 No. 3, pp. 593-616.

Orlikowski, W.J. and Iacono, C.S. (2001), "Research commentary: desperately seeking the 'IT' in IT research – a call to theorizing the IT artifact", *Information Systems Research*, Vol. 12 No. 2, pp. 121-134.

Oxley, J.E. (1999), "Institutional environment and the mechanisms of governance: the impact of intellectual property protection on the structure of inter-firm alliances", *Journal of Economic Behavior & Organization*, Vol. 38 No. 3, pp. 283-309.

Patton, M.Q. (2002), *Qualitative Research & Evaluation Methods*, 3rd ed., Sage, Thousand Oaks, CA.

Pawlowski, J.M., Bick, M., Peinl, R., Thalmann, S., Maier, R., Hetmank, L., Kruse, P., Martensen, M. and Pirkkalainen, H. (2014), "Social knowledge environments", *Business & Information Systems Engineering*, Vol. 6 No. 2.

Podsakoff, P.M., Mackenzie, S.B., Lee, J.Y. and Podsakoff, N.P. (2003), "Common method biases in behavioral research: a critical review of the literature and recommended remedies", *Journal of Applied Psychology*, Vol. 88 No. 5, pp. 879-903.

Quintas, P., Lefrere, P. and Jones, G. (1997), "Knowledge management: a strategic agenda", *Long Range Planning*, Vol. 30 No. 3, pp. 385-391.

Randeree, E. (2006), "Knowledge management: securing the future", *Journal of Knowledge Management*, Vol. 10 No. 4, pp. 145-156.

Rowley, J. and Slack, F. (2004), "Conducting a literature review", *Management Research News*, Vol. 27 No. 6, pp. 31-39.

Schultze, U. and Leidner, D.E. (2002), "Studying knowledge management in information systems research: discourses and theoretical assumptions", *MISQ*, Vol. 26 No. 3, pp. 213-242.

Seidel, S., Müller-Wienbergen, F. and Becker, J. (2010), "The concept of creativity in the information systems discipline: past, present, and prospects", *Communications of the Association for Information Systems*, Vol. 27, pp. 217-242.

Snyder, H. and Crescenzi, A. (2009), "Intellectual capital and economic espionage: new crimes and new protections", *Journal of Financial Crime*, Vol. 16 No. 3, pp. 245-254.

Teece, D.J. (1986), "Profiting from technological innovation: Implications for integration, collaboration, licensing and public policy", *Research Policy*, Vol. 15 No. 6, pp. 285-305.

Thalmann, S., Manhart, M., Ceravolo, P. and Azzini, A. (2014), "An integrated risk management framework: measuring the success of organizational knowledge protection", *International Journal of Knowledge Management*, Vol. 10 No. 2, pp. 28-42.

Trkman, P. and DeSouza, K.C. (2012), "Knowledge risks in organizational networks: an exploratory framework", *Journal of Strategic Information Systems*, Vol. 21 No. 1, pp. 1-17.

Tuomi, I. (1999), "Data is more than knowledge: implications of the reversed knowledge hierarchy for knowledge management and organizational memory", *Journal of Management Informatio Sustems*, Vol. 16 No. 3, pp. 107-121.

Upadhyaya, S.J., Rao, H.R. and Padmanabhan, G. (2011), "Secure knowledge management", in Schwartz, D. and Te'eni, D. (Eds), *Encyclopedia of Knowledge Management*, 2nd ed., Information Science Reference, Hershey, PA.

Urcuyo, C. and Kunnathur, A. (2002), "Knowledge sharing strategy: the significance of security and collaboration", *AMCIS 2002 Proceedings, Paper*, *Dallas, Texas*.

Väyrynen, K., Hekkala, R. and Liias, T. (2013), "Knowledge protection challenges of social media encountered by organizations", *Journal of Organizational Computing and Electronic Commerce*, Vol. 23 No. 1, pp. 34-55.

von Krogh, G. (2012), "How does social software change knowledge management? Toward a strategic research agenda", *The Journal of Strategic Information Systems*, Vol. 21 No. 2, pp. 154-164.

Webster, J. and Watson, R.T. (2002), "Analyzing the past to prepare for the future: writing a literature review", *MISQ*, Vol. 26 No. 2, pp. 13-23.

Williamson, O.E. (1985), *The Economic Institutions of Capitalism*, Free Press, New York, NY.

Zhou, X. and Liu, Y. (2010), “Toward proactive knowledge protection in community-based software development”, *Proceedings of the 2010 ICSE Workshop on Cooperative and Human Aspects of Software Engineering, ACM*, *Cape Town*, pp. 76-83.

About the authors

Markus Manhart holds an MSc in Information Systems from the University of Innsbruck, Austria. Since November 2010, he is working as a researcher at the Information Systems Unit of the University of Innsbruck, School of Management, and he is currently involved in the EU FP7 research projects “PoSecCo” and “Learning Layers”. He is also working on his PhD focussing on knowledge protection in business networks. Markus Manhart is the corresponding author and can be contacted at: markus.manhart@uibk.ac.at

Stefan Thalmann holds a PhD in Information Systems from the University of Innsbruck, Austria. He worked as researcher at the Martin-Luther-University of Halle-Wittenberg, Germany, and as visiting researcher at the London Metropolitan University, UK, and at the University of Jyväskylä, Finland, and is currently employed as an Assistant Professor at the University of Innsbruck. He has published articles in journals and conference proceedings on knowledge management and knowledge protection, information security and compliance management, as well as on technology-enhanced learning.

This article has been cited by:

1. SerenkoAlexander Alexander Serenko Dr Alexander Serenko is based at the Faculty of Business Administration, Lakehead University, Thunder Bay, Canada. He is a Professor of Management Information Systems in the Faculty of Business Administration at Lakehead University, Canada. Dr Serenko holds a PhD in Management Information Systems from McMaster University. His research interests pertain to scientometrics, knowledge management and technology addiction. Alexander has published over 70 articles in refereed journals, including MIS Quarterly, European Journal of Information Systems, Information & Management, Communications of the ACM and Journal of Knowledge Management. He has also won six Best Paper awards at Canadian and international conferences. In 2015, Dr Serenko received the Distinguished Researcher Award which is the highest honor conferred by Lakehead University for research and scholarly activity. BontisNick Nick Bontis Dr Nick Bontis is based at the DeGroote School of Business, McMaster University, Hamilton, Canada. He is Chair of Strategic Management at the DeGroote School of Business, McMaster University. He received his PhD from the Ivey Business School at Western University. He is the first McMaster Professor to win Outstanding Teacher of the Year and Faculty Researcher of the Year simultaneously. He is a 3M National Teaching Fellow, an exclusive honour only bestowed upon the top university professors in Canada. He is recognized the world over as a leading professional speaker and a consultant. Faculty of Business Administration, Lakehead University, Thunder Bay, Canada DeGroote School of Business, McMaster University, Hamilton, Canada . 2016. Understanding counterproductive knowledge behavior: antecedents and consequences of intra-organizational knowledge hiding. *Journal of Knowledge Management* **20**:6, 1199-1224. [Abstract] [Full Text] [PDF]
2. MassaroMaurizio Maurizio Massaro Maurizio Massaro is Lecturer at the Department of Economic Sciences and Statistics, University of Udine, Udine, Italy. He, PhD, has been an Assistant Professor at Udine University since 2008. Before joining academia, he was founder and CEO of multiple consultancy firms. He has also served as a research center Vice President in the field of metal analysis. He has been a visiting Professor at Florida Gulf Coast University and Leicester University. He enjoys several contacts and research partnerships with universities in the USA, continental Europe, the UK and Australia. His research interests include knowledge management, intellectual capital, sustainability in international business and research methods. HandleyKaren Karen Handley Karen Handley is Postdoctoral Research Fellow at the Department of Accounting and Corporate Governance, Macquarie University, Sydney, Australia. She is a Postdoctoral Research Fellow in the Department of Accounting and Corporate Governance at Macquarie University in Sydney, where she has been employed since completing her PhD in Accounting in 2013. An MBA Old Mutual Gold Medallist from the University of Cape Town, Karen's roles prior to academia included owner manager of various small businesses in Canada and Australia, and Information Technology project management in the mining and retail industries. Karen's research interests are grounded in real-world financial accounting and corporate governance issues, with a particular focus on small and medium-sized entities. BagnoliCarlo Carlo Bagnoli Carlo Bagnoli is Associate Professor at the Department of Management, Ca' Foscari University of Venice, Venice, Italy. He is Associate Professor of Business Policy and Strategy at the Department of Management, Ca' Foscari University of Venice. He received a PhD in Business Economics at Ca' Foscari University of Venice. He was a visiting research fellow at the University of Florida. He is Scientific Director of the Innovarea Project funded by the Regional Italian Government. His research interests include knowledge management, competitive strategy and business model innovation. Carlo's research work has been published in various outlets, including the Journal of Business Economics and Management, Industrial Management & Data System, Journal of Management and Governance and Journal of Intellectual Capital. DumayJohn John Dumay John Dumay is Associate Professor of Accounting at the Department of Accounting and Corporate Governance, Macquarie University, Sydney, Australia. He is an Associate Professor in Accounting at Macquarie University, Sydney. He worked for over 15 years as an independent business consultant across a wide variety of industries before joining academia after completing his PhD in 2008. His PhD entitled Intellectual Capital in Action: Australian Studies won the prestigious Emerald/EFMD Outstanding Doctoral Research Award for 2008 for the Knowledge Management category. John continues to research on the topic of intellectual capital, sustainability reporting, innovation, research methods and academic writing. His research activities link closely to management accounting and scholarly practice. Department of Economic Sciences and Statistics, University of Udine, Udine, Italy. Department of Accounting and Corporate Governance, Macquarie University, Sydney, Australia. Department of Management, Ca' Foscari University of Venice, Venice, Italy. Department of Accounting and Corporate Governance, Macquarie University, Sydney, Australia.. 2016. Knowledge management in small and medium enterprises: a structured literature review. *Journal of Knowledge Management* **20**:2, 258-291. [Abstract] [Full Text] [PDF]
3. Sarigianni Christina, Thalmann Stefan, Manhart MarkusProtecting Knowledge in the Financial Sector: An Analysis of Knowledge Risks Arising from Social Media 4031-4040. [CrossRef]
4. Ilona Ilvonen, Aki Alanne, Nina Helander, Hannele VayrynenKnowledge Sharing and Knowledge Security in Finnish Companies 4021-4030. [CrossRef]