Towards a Business-Driven Process Model for Knowledge Security Risk Management: Making Sense of Knowledge Risks

International Journal of Knowledge Management

October-December 2015, Vol. 11, No. 4

Table of Contents

Special Issue on Knowledge Management and Risk

Editorial Preface

Research Articles

The *International Journal of Knowledge Management* is indexed or listed in the following: ACM Digital Library; Australian Business Deans Council (ABDC); Bacon's Media Directory; Burrelle's Media Directory; Cabell's Directories; Compendex (Elsevier Engineering Index); CSA Illumina; DBLP; DEST Register of Refereed Journals; Gale Directory of Publications & Broadcast Media; GetCited; Google Scholar; INSPEC; JournalTOCs; KnowledgeBoard; Library & Information Science Abstracts (LISA); MediaFinder; Norwegian Social Science Data Services (NSD); PsycINFO®; SCOPUS; The Index of Information Systems Journals; The Standard Periodical Directory; Ulrich's Periodicals Directory

Towards a Business-Driven Process Model for Knowledge Security Risk Management:
Making Sense of Knowledge Risks

Ilona Ilvonen, Tampere University of Technology, Tampere, Finland

Jari J Jussila, Tampere University of Technology, Tampere, Finland

Hannu Kärkkäinen, Tampere University of Technology, Tampere, Finland

ABSTRACT

The purpose of this paper is to introduce a model to manage knowledge security risks in organizations. Knowledge security risk management is a sensemaking process that should be carried out by managers, and the proposed model works as a tool for the sensemaking process. The model is illustrated with an analytical case example. The process model helps to identify knowledge security risks and provides a comprehensive approach to evaluating and balancing the costs and benefits of knowledge sharing and knowledge risk management. The paper addresses calls for research on the emerging topic of knowledge security and the important topic of new knowledge sharing tools from the combined perspectives of business benefits and risk management. The results presented in this paper are preliminary and conceptual, and further research on the topic is suggested. The process model proposed in this paper can be a valuable tool for practitioners aiming to develop knowledge sharing practices in companies, and at the same time need to consider the security of knowledge.

Keywords: *Knowledge Protection, Knowledge Risks, Knowledge Sharing, KSRM, Sensemaking, Tampere University of Technology*

INTRODUCTION

Knowledge and its creation are important sources of competitive advantage and business opportunities for most contemporary organizations (Alavi & Leidner, 2001; Choo, 1996; Grant, 1996; Nonaka & Takeuchi, 1995). Although knowledge creation, sharing and management have been researched extensively (e.g. Bolisani & Scarso, 2014; Matayong & Mahmood, 2013; Tzortzaki & Mihiotis, 2014), there is one viewpoint to knowledge that has received less attention: knowledge security (Randeree, 2006; Shedden, Scheepers, Smith, & Ahmad, 2011). Despite the importance

DOI: 10.4018/IJKM.2015100101

of knowledge and the need for knowledge protection, there is little literature on knowledge security (Shedden et al. 2010). In terms of knowledge security and risk analysis, most existing risk analysis methods can be regarded as providing a plain technical view on information and technological assets (Ahmad, Bosua, & Scheepers, 2014; A.M. Padyab, Paivarinta, & Harnesk, 2014; Shedden et al., 2011; Shedden, Smith, & Ahmad, 2010; Spears, 2006), ignoring that knowledge is bound to people (Shedden et al., 2010, 2011; Ilvonen, 2013; A.M. Padyab et al., 2014) and as a consequence people (Ilvonen, 2013; Trkman & Desouza, 2012; Shedden et al., 2011, 2010; Spears, 2006; Siponen, 2000; Spruit & Looijen, 1996) and especially their communication (Ilvonen, 2013; Padyab et al., 2014) are significant sources of knowledge security risks.

Since knowledge security risks have not received extensive attention in the existing literature (M. Jennex, 2014), there is need to look also for parallel fields in order to understand the principles of security risk management. Information security risk assessment (ISRA) methodologies are means by which organizations aim to manage information security risks (Baskerville, 1991; Siponen, 2005; Whitman & Mattord, 2011). However, typical perspectives on information security risk management, including most ISRA methodologies, largely ignore the business context of information systems (Shedden et al., 2010; Spremic, 2012), and are not framed in terms of competitive advantage (Ahmad et al., 2014). When the business perspective is considered (DeLoach, 2004; Siponen, 2005; Von Solms & Von Solms, 2004), it is mainly limited to the evaluation of individual risk mitigation techniques and their cost reasoning, rather than starting from a broad perspective of reasoning the business benefits of an activity compared to the risks connected to it.

This paper aims to answer the research question "How can organizations manage knowledge security risks in a proactive business-driven way?" The authors argue that knowledge security risks should be managed in a systematic process, and introduce a conceptually developed process for this purpose. This paper extends the line of research opened up by several authors (Ahmad et al., 2014; Aljafari & Sarnikar, 2009; Desouza & Vanapalli, 2005; A.M. Padyab et al., 2014; Shedden et al., 2011; Siponen & Oinas-Kukkonen, 2007) and answers to calls for research on the specific area of knowledge security.

Several studies point out that increasing the circulation of knowledge also increases the risk of leakage (Desouza, 2006; Desouza & Vanapalli, 2005; Easterby-Smith, Lyles, & Tsang, 2008; Trkman & Desouza, 2012). New forms of organizational operation, such as open innovation and different uses of social media, emphasize opening up of organizational knowledge resources towards customers and other organizational stakeholders. Therefore, when making changes in practices, there is simultaneously a strong need for understanding the potential risks related to open information and knowledge flows, as well as relating these risks to the potential business benefits of the change.

After introducing the theoretical background, the paper introduces the proposed process model and discusses the relation of the process steps to previous work. After this an analytical case that illustrates the outputs of the process model from a practical perspective is presented. The paper concludes with a brief discussion on avenues for further research.

THEORETICAL BACKGROUND

Knowledge

In this paper the term knowledge is understood as an intangible asset that is mainly possessed and created by people (Nonaka & Takeuchi, 1995). Knowledge is a result of human thinking and interpretation (Davenport & Prusak, 1998; Thierauf, 2001). Although knowledge in most cases is embedded in people as tacit knowledge, that knowledge can be to some extent shared with

other people by externalizing it into a form of explicit knowledge, i.e. written or spoken language (Nonaka & Takeuchi, 1995; Szulanski, 2000). Knowledge generates value to a company through its use and sharing; this requires that the people receiving knowledge are able to interpret the shared knowledge, and use it for learning and reflection (Alavi & Leidner, 2001). Knowledge thus is of value to an organization when the right people have and use the correct knowledge.

When a company creates competitive advantage from the knowledge of its workers, the knowledge becomes the biggest asset of the company (Grant, 1996). This idea is the backbone of the "knowledge-based view" of the firm (Kogut & Zander, 1992; Spender & Grant, 1996). When knowledge is considered a resource of an organization, it is considered bound to the individual people that have it, but also something that is possible to transfer from person to person (Hansen, 1999) on individual and collective (Krogh, 2009) levels. While knowledge is used for making sense of the situation the organization is in, the organization also creates new knowledge and makes decisions based on that knowledge (Choo, 1996). This makes knowledge an elusive object to secure, since new knowledge is created all the time. In fact, the process of knowledge security risk management is in itself a process of new knowledge creation, which the paper will discuss further when the process model is presented.

Knowledge Security

The use and sharing of knowledge requires communication between people that possess the knowledge (Hansen, 1999; Nonaka & Takeuchi, 1995). Today there are numerous technical tools to support discussion and knowledge sharing, among them different information systems and social media tools that are designed to mimic face-to-face communication between people that are possibly geographically apart (von Krogh, 2012). From the point of view of knowledge, these kind of tools are repositories for knowledge (Aljafari & Sarnikar, 2009) in addition to being channels for knowledge exchange (Padyab et al., 2014). A systematic way to identify and manage risks connected to knowledge would help in establishing a unified level of protection of knowledge, but research shows that this does not exist, at least not widely in organizations (Ahmad et al., 2014). Knowledge security or knowledge protection are not unaddressed in the literature, but individual processes concentrate on narrow areas of knowledge security, such as securing knowledge of leaving employees (Jennex, 2014) or concentrating on more formal protection mechanisms (Olander, Vanhala, & Hurmelinna-Laukkanen, 2014).

The concept of knowledge security (Desouza, 2006; Ryan, 2006; O'Donoghue & Croasdell, 2009; Ilvonen, 2013; Padyab et al., 2014) is established in the information security management and knowledge management fields, but it does not yet have a commonly used definition (Ilvonen, 2013; Jennex & Durcikova, 2014; Shedden et al., 2011). In this paper knowledge security is understood as the managerial process of organizations to identify threats toward important knowledge and secure the knowledge against those threats. As knowledge is bound to people, knowledge security is closely related to managing people and their activities both within an organization and across organizational boundaries.

Risk Management

Risk as a term refers to an event that may have great consequences to an organization, but that is uncertain to happen. In financial terms risk can be understood as either a positive or negative event (DeLoach, 2004). Especially business risks always have the potential of positive financial outcomes. However, this paper concentrates on knowledge risks that, if realized, have negative consequences to an organization. These two, however, are intertwined and cannot be entirely

separated from each other, especially when cost-benefit analysis is added as an essential element to risk management.

A risk is constructed of several components: a threat, the consequences of the realization of that threat, and the probability of the realization (M. E. Jennex & Zyngier, 2007; Stoneburner, Goguen, & Feringa, 2002). Knowledge risks may harm an organization for example by reducing competitive advantage, by damaging the reputation of a company or by creating distress among employees (Ali Mohammad Padyab, Päivärinta, & Harnesk, 2014; Väyrynen, Hekkala, & Liias, 2013). Knowledge risks can be seen to originate either from external sources or from internal sources (Ilvonen, 2013; Markus Manhart & Thalmann, 2015). The division to external and internal threats in the context of this paper refers to whether there are external actors involved in the realization of a threat. In case of knowledge risks the vulnerabilities that cause threats and consequently risks can be numerous, and they all have a human element in them, since the knowledge is bound to people.

Generally, four basic phases can be identified from risk management processes. These are for example (e.g. Lichtenstein, 1996; Bandyopadhyay, Mykytyn, & Mykytyn, 1999):

- Asset and risk identification;
- Risk analysis;
- Risk-reducing measures; and
- Risk monitoring.

The main steps can be found also from many information security risk management models (Caralli, Stevens, Young, & Wilson, 2007; Shedden et al., 2011). The steps in the process may get different names from different authors, but the essential content of the process remains the same. What is common to the security risk management processes is that many times the trigger to begin a risk management process comes from the reason that risk management requirements and standards need to be met (Webb, Maynard, Ahmad, & Shanks, 2013; Thalmann, Manhart, Ceravolo, & Azzini, 2014; Markus Manhart & Thalmann, 2015).

Project risk management literature considers risk management to be triggered by the need of a development project (e.g. Varnell-Sarjeant, 2008; Jafari, Rezaeenour, Mazdeh, & Hooshmandi, 2011). The focus of project risk management, however, is usually that of successful completion of the project; within deadline and within budget. Security risks get less attention in the project management process models. The idea of the process model presented in this paper is to combine the approaches of project risk management and security risk management to get a comprehensive approach to identify, manage and monitor knowledge security risks.

A PROCESS MODEL FOR KNOWLEDGE SECURITY RISK MANAGEMENT

The knowledge security risk management process model (KSRM) is illustrated in Figure 1. Although the authors acknowledge that no risk management model can cover all risks, all activities and all information or knowledge (Marabelli & Newell, 2012; Trkman & Desouza, 2012) they try to incorporate a wide understanding of the risk management process steps into the KSRM model.

This paper concentrates on discussion of the knowledge management contributions of the risk management process steps. One key knowledge management model discussed along the risk management model is presented by Choo (1996) and illustrated in Figure 2.

Figure 1. Knowledge security risk management (KSRM) process

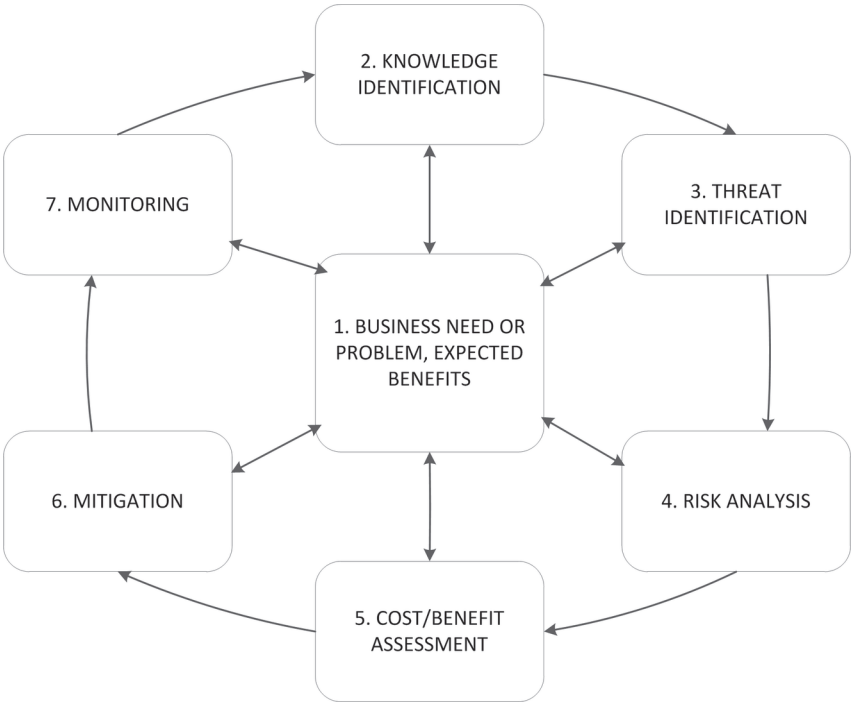
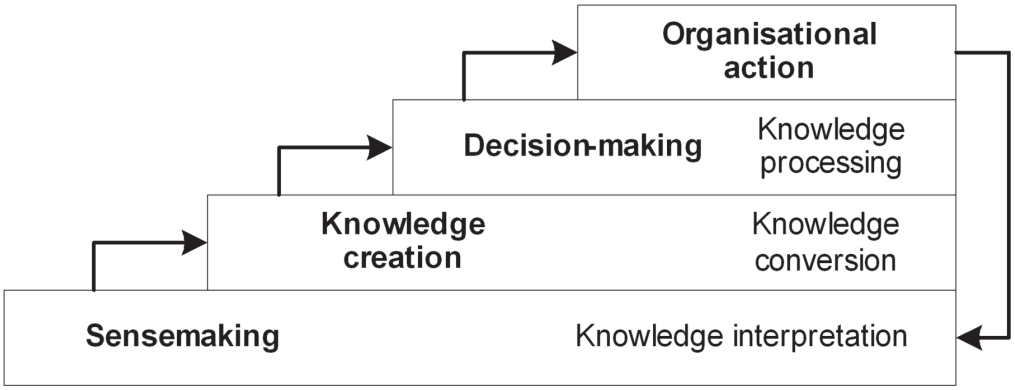


Figure 2. Model of sensemaking and knowledge creation, modified from Choo (1996)



Step 1: Business Need

Existing KSRM models do not discuss much what should trigger the process, or their perspective towards business goals. The few links to business include: focusing on processes critical for business (Shedden et al., 2011, 2010), concentrating on stakeholders who are perceived important according to organizational strategic goals and objectives (Padyab et al., 2014), identifying strategic assets related to key business processes and involving organization's members and external

partners involved in those business processes in the knowledge risk management process (Aljafari & Sarnikar, 2009), supporting reduction of transaction costs in inter-organizational collaboration by making explicit both risks and knowledge transfer benefits (Trkman & Desouza, 2012), and ensuring that knowledge protection meet requirements forced by laws, standards, customers or internal regulations (M. Manhart & Thalmann, 2013).

The KSRM process illustrates a continuous process that is triggered by a business goal, need or problem that needs to be solved (center of Figure 1). The process may be triggered by changes in the operations or environment of the company. In this step the goals and benefits sought from the change need to be defined, as well as the people that are responsible for the realization of those benefits (Ward & Daniel, 2006) and the evaluating of the risks.

The KSRM process is one example of a process that creates new knowledge in organizations. The first step of the process should include an element of sensemaking: understanding the business situation the organization is in, and what is going on around it. An organization should constantly aim at making sense of the business situation and its surroundings (Choo, 1996). Although Choo's model in Figure 2 in one way is connected to each of the following steps of the knowledge security risk management model, sensemaking is something that companies should do with every intended business change. Sensemaking refers to an organization actively figuring out what kind of knowledge is available to it, what is the situation surrounding the organization, and what this situation means for it (Choo 1996).

The output of the first step of the KSRM process is the business case of the intended change and a description of what kind of benefits are sought by the change.

Step 2: Knowledge Identification

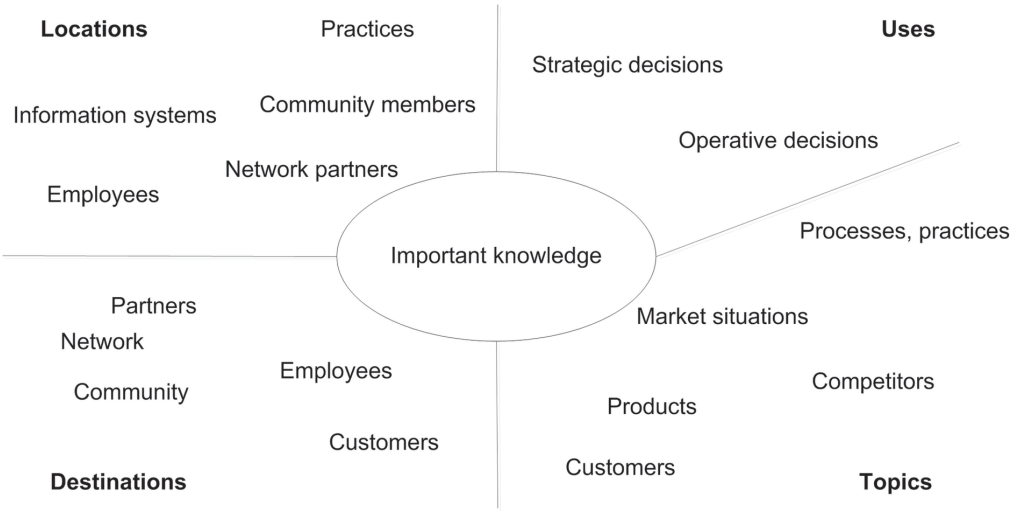
The first step in the generic risk management process and the second step of the KSRM process is to identify important knowledge that may be at risk in the organization. There are various approaches to knowledge asset identification (e.g. Padyab et al., 2014; Shedden et al., 2011; Trkman & Desouza, 2012). Knowledge is bound to people, and there is a lot of knowledge that each individual possesses. However, not all that knowledge is important to the organization.

One way to structure and identify knowledge is to examine different locations, uses, topics and destinations of knowledge to identify knowledge assets, and to prioritize between them (Ilvonen 2013). These dimensions are illustrated in Figure 3. The dimensions are one way to ensure that the organization has a broad enough scope when they begin to identify important knowledge that needs to be secured. The knowledge identification phase is still part of the sensemaking describes in Choo's (1996) model (Figure 2).

Another way to approach identification of important knowledge is to use the genre-based method for identifying knowledge assets (A.M. Padyab et al., 2014). In this method knowledge is recognized through identifying actors who communicate within the organization. The different types of communication between different actors form genres of knowledge, that is, in Figure 3, the interaction between the locations and destinations of knowledge. This method is useful in locating knowledge, as well as recognizing the ways and tools that it is communicated with, as it covers all; locations, destinations, topics and uses of knowledge illustrated in Figure 3.

A method for identification of knowledge assets is also to examine the containers or reservoirs where the knowledge resides (Caralli et al., 2007; Aljafari & Sarnikar, 2009). This can mean either people, as with knowledge is obvious, but also for example social media tools and other information systems that are used for documenting and sharing of knowledge (Aljafari & Sarnikar, 2009). Important knowledge exists both in the individual and collective level (Krogh, 2009) and this should be acknowledged in the identification step.

Figure 3. Identification of important knowledge



In moments of change and development the questions that need to be asked to identify the important knowledge depend on the context. For example, if the KSRM process is applied to the context of implementing new social media tools, identification can be performed by answering e.g. the following questions:

- What knowledge will be shared with the tool?
- Who will be using the tool?
- For what purposes will different stakeholders use the social media tool?
- What is the importance of the knowledge that is shared within the social media tool?

The purpose of the knowledge identification step in this context is to gain an understanding of what knowledge will be shared over the chosen social media platform (Braun & Esswein, 2012; von Krogh, 2012), what is the construction of the community that will be using it, and what significance the knowledge holds for the company/companies that collaborate in the platform (Haefliger, Monteiro, Foray, & von Krogh, 2011).

The output of the knowledge identification step is an inventory of important knowledge, a list of people that are users or holders of that knowledge, and a list of communication media that are used for sharing that knowledge. The knowledge identification step of risk management can be conducted parallel to the knowledge management process of the organization.

Step 3: Threat Identification

The third step of the KSRM process is threat identification. Many authors (Aljafari and Sarnikar 2009; Padyab et al. 2014; Shedden et al. 2011; Trkman and Desouza 2012) include threat identification either as an individual process phase or as a part of the risk analysis phase in knowledge security risk management process. One includes also a method and a tool for identifying threats related to knowledge assets: the Octave Allegro method and it's worksheets (Padyab et al. 2014).

A threat is the potential of a negative event (Caralli et al., 2007). It can be further broken down into a vulnerability, an actor or a threat agent that exploits that vulnerability, a motive that the actor has to the exploitation and the outcome of the event (Caralli et al., 2007; Farahmand, Navathe, Enslow, & Sharp, 2003). In order to identify threats to knowledge, an organization needs to recognize vulnerabilities connected to protecting that knowledge, as well as potential actors that threaten the knowledge along with their motives.

One suggestion for performing identification of threats to information is to use standards and ready-made checklists, instead of a deeper down analysis of vulnerabilities and threat agents (e.g. Farahmand et al., 2003; Caralli et al., 2007; Peltier, Peltier, & Blackley, 2005). In addition to just relying on standards and checklists, the step can be performed for example by creating typical and non-typical knowledge use and communication scenarios, and identifying potential threats from these scenarios (Caralli et al., 2007; Peltier et al., 2005).

The scope of the threats is one aspect that needs to be considered when threats are identified: threats may apply only to a limited part of an organization, to the entire organization and in severe situations also to other organizations (Trkman & Desouza, 2012). Especially with knowledge, the target and outcome of threats may be both intangible, so it is not necessary to categorize threats for example to natural, environmental or human threats (Farahmand et al., 2003). Instead, a division to external threats and accidental or deliberate internal threats may be more useful (Trkman & Desouza, 2012) along with the analysis of the result of the threats. The outcome of knowledge threats may, for example, directly benefit a competitor by revealing critical competitive knowledge (Ahmad et al., 2014), or indirectly harm the organization by affecting the trust of customers (Braun & Esswein, 2012). This stage begins the knowledge creation stage presented in Figure 2 (Choo, 1996) since the threats are identified both through the use of previous knowledge and through brainstorming for organization-specific threats.

In the example case of social media understanding is needed of both, the technical properties of the social media platform, and the operations of the community that uses the platform, to create understanding of the threat agents and scenarios. The threats can be caused from sources outside the community e.g. a competitor company aspiring to get strategic knowledge of product development, or from sources inside the company, e.g. a careless employee misusing the social media platform. In the case of knowledge, the main vulnerability is that knowledge may be beneficial to a competitor.

The outcome of the threat identification step is an analysis of what threatens the important knowledge of the organization, and what are the sources of threat agents of those threats.

Step 4: Risk Analysis

The fourth step of the KSRM process is risk analysis. In this step the threats identified in the previous step are individually analyzed to understand what kind of risks they cause and how significant these risks are to the organization. Several models discuss risk analysis as a process phase in knowledge security risk management (Aljafari and Sarnikar 2009; Padyab et al. 2014; Trkman and Desouza 2012). Aljafari & Sarnikar (2009) include sub-phases of making assertions, providing evidence to support them, and calculating risk in the risk analysis process phase and propose the Demspter-Shaefer (Dempster 1967; Shafer 1976) model as an approach for performing the risk analysis. Trkman & Desouza (2012) introduce a framework that categorizes knowledge-sharing risks and propose that managers can use the framework as a guide/sense-making device in identifying the main types of risk facing their organization. The Octave Allegro (Caralli et al. 2007) method introduced in Padyab et al. (2014) provides an approach and a tool for both

identifying the threats and vulnerabilities and deciding on the risk mitigation actions (mitigating risks, transferring risks, avoiding risk, or accepting risk).

A risk is the combination of two elements: the consequences of a threat and the probability of it (Stoneburner et al., 2002; Peltier et al., 2005). In this step knowledge of the consequences of a threat is essential, yet difficult to gain (Aljafari & Sarnikar, 2009). In many cases, exact monetary figures to the consequences of a threat are difficult to calculate. In addition to that, the exact probability of a threat is rarely known. Thus, to simplify the risk analysis process a 3x3 or 4x4 matrix with threat consequences categorized from severe to minor and the probability categorized from certain to highly unlikely can be used to assess whether the risks are major or minor (Stoneburner et al., 2002; Caralli et al., 2007). The matrix works as a tool to help prioritize between risks that are too severe to accept as such, and thus should be mitigated, and risks that are small enough to accept. However, since the risks are elusive in terms of exact numbers for probability and consequences, the risk analysis matrix should be used as a tool for collective sensemaking of the magnitude of the knowledge risks the organization is facing. In this step all the steps of Choo's model are performed, since in addition to sensemaking and knowledge creation, decisions regarding the risks need to be made.

In the example context of social media, in this step the calculations that have been done to prove the business case of implementing the social media platform can be useful, since many threats would result in the loss of the aspired benefits. In many cases, however, the loss of benefits would not be an accurate estimate of the consequences or damages a threat would result in. For example, the leaking of critical knowledge can lead to loss of trust of customers, which in turn can have greater consequences than just the loss of benefits of one knowledge sharing project.

The output of the risk analysis phase is a list of identified risks that are associated with the business activities of the organization. The risks are prioritized based on the estimated probability and severity.

Step 5: Cost-Benefit Analysis

The next step, the cost-benefit-analysis, is an essential step of risks management. Elements of this step are performed all along the risk management process, yet it needs to be acknowledged as an individual step in the process in order to systematize the activity. The step gets substantial input from the risk analysis step, but also from the earlier steps of the process, as well as from other sources such as the business case that was built to support the implementation of the change at hand. The cost-benefit analysis gathers together all the benefits and positive elements and all the costs and risks that are connected to the implementation of the social media platform. This step should include the discussion of different managers so that the costs and benefits are thoroughly weighed.

The key of this step is to involve both the owners of benefits of changes as well as the owners of the risk management of the change in the sensemaking of the costs and benefits. This enables the organisation to weigh the total costs of the implementation against the total expected benefits. The difficulty with risk management is typically that the costs of mitigation are weighed only against the value of individual knowledge assets. Asset valuation is difficult at best, and the value of an asset is tied to the benefits that asset can generate when used. The knowledge risk management cost-benefit assessment tries to address the benefits of a possible change in comparison to the costs of the change, and the possible cost of risks involved with the change. In the example context of social media use in organizations this means that in addition to considering the benefits of use of knowledge and the benefits of the new work processes, the costs of implementing the social media platform and the costs of potential risks and their mitigation

are discussed together. The risk analysis process requires discussion, and the discussion should continue at the cost-benefit analysis stage in order to achieve a common understanding of the sought benefits and risks that are associated with them. In situations where there are alternative solutions to the business problem or change, the cost-benefit-analysis can also compare the benefits, risks and costs of the current situation with the expected benefits, risks and costs brought on by the change. For example, if a social media platform is used for knowledge sharing, the costs and risks of the use of this platform can be compared with the costs and risks of the current solution (e.g. email messages and face-to-face conversations).

The output of the cost-benefit analysis is an analysis of what are the costs of implementing the change and mitigating the risks of the change. Depending on the result of the analysis decision can be made whether to go on with the implementation process, or make changes to the approach.

Step 6: Risk Mitigation

Risk mitigation is addressed by several authors also in literature on knowledge risk management (Aljafari & Sarnikar, 2009; Padyab et al., 2014; Shedden et al., 2011; Thalmann et al., 2014). Aljafari & Sarnikar (2009) propose developing security policies as the primary means of mitigating risks. Shedden et al. (2011) propose the SECI model (Nonaka & Takeuchi, 1995) of socialization, externalization, combination and internalization as a way to mitigate knowledge risks (Shedden et al., 2011). Thalmann et al. (2014) suggest internal knowledge audits as means of risk mitigation by auditing the performance metrics of knowledge protection controls.

Risk mitigation is begun at the previous stages, when the risks too big to accept, but possible to mitigate are identified. The implementation of risk mitigation controls adds to the costs, but on the other hand diminishes risks, and may thus affect the balance between costs and benefits. Mitigation controls may affect the consequences of a threat, e.g. the knowledge that is shared within a social media platform is strictly limited to non-strategic knowledge, and thus the consequences of a leak are reduced. Or the controls may reduce the probability of a threat. For example, the number of people that have administrator privileges to a platform is reduced to a minimum to reduce the odds of accidental misconfiguration. Typical social media risk mitigation controls include implementing a social media policy and training of employees in proper use of the social media platform. Technical controls that limit for example the use of certain social media platforms would be another example of a control.

Risk mitigation controls need to be selected after a careful consideration of which risks are worth addressing, and when mitigation is reasonable. The risk analysis and cost-benefit assessment may also result in decisions that render risk mitigation unnecessary, if the change is abandoned because it will not provide enough benefits. On the other hand, the cost-benefit assessment may prove some mitigation choices too costly, and result in selection of other, less costly, means of mitigation.

The output of the mitigation step is a list of risk controls that need to be implemented, and a plan for implementing them. The output also identifies risks that are accepted, i.e. they are not mitigated. However, the mitigation plan may include contingency plans for the potential realization of the accepted risks.

Step 7: Monitoring

The last, seventh, step in the risk management model is monitoring. Although this is identified as one key step in the general risk management literature (Liechtenstein 1996), most knowledge risk management models do not explicitly discuss monitoring. As one approach knowledge security is proposed to be monitored with of knowledge audits (Thalmann et al., 2014).

This step includes the monitoring of the threat environment, as well as the monitoring of the use of knowledge, which translate to another sensemaking, knowledge creation, decision making and organizational action phases of Choo's model (Choo 1996, Figure 2). Any changes in the use habits, users, shared knowledge, purpose and technological environment should trigger a re-assessment of the threats and risks that are connected to the activity that initially was processed in the risk management model.

In the example of the social media, monitoring can include for instance setting up certain measurements and alarm threshold for those measurements that, when reached, will trigger an alarm and enable the organization to react to the threat as quickly as possible. For example, sentiment analysis can be used to evaluate the sentiment of the conversations about the company and its products and services in order to determine whether the conversations are positive, negative or neutral. An alarm can be triggered from e.g. each negative conversation or when reaching a defined alarm triggering level of sentiment of the conversations, or some other set alarm-related indicator which might indicate a risk to be taking place in the near or further future.

The output of the monitoring step of risk management is situational awareness of the risk environment of the organization. This step ties the knowledge security risk management process to other managerial processes of the organization.

ILLUSTRATIVE CASE

This paper proposes a new process model for managing knowledge security risks in organizations. In this section this model is applied to an open innovation, crowdsourcing case, to illustrate how the model works. This case is one example of the kind of contexts this model can be applied to, and this is why it is presented in a general level. The case company is a globally operating manufacturing company, and various internal company functions were involved in knowledge sharing. In addition to this, a crowdsourcing platform provider, an industrial community and individual professionals were involved in the case. The KSRM process is applied to the case analytically, i.e. after the events took place.

The focal company of the case needed to develop a new component to ensure and monitor safe operation of their new core product. The component itself is an independent product that complements the main product. The company decided to gather fresh ideas for this component through crowdsourcing in an open innovation challenge. In addition to this challenge the company decided to schedule development sprints for the component immediately after the open challenge. This way they ensured that the results of the challenge would be taken further without delay. The knowledge security risk management process connected to this open innovation process is described in Table 1.

In Table 1 the main benefit that the focal company sought from the crowdsourcing was fresh and innovative ideas with minimal consumed resources. The threat and risk analysis steps emphasize the biggest threat of this open innovation endeavor: the competitors will find out what the company is planning to do. There was significant consideration on what component of the product could be opened up for the challenge. The main reason that tilted the cost-benefit scale toward the benefit-side in this case was the non-strategic nature of the component that was developed through open innovation. The component is vital for the safety of the product, but it is not strategic for the focal company.

Table 1. Example of KSRM process outputs

No	Step	Outputs in the Example Case
1	Business need	**Trigger and business need:** Need to develop a new component for monitoring safety and maintenance need of a product Need for more product development resources -> decision to crowdsource ideas from engineering community **Expected benefits:** Faster innovation process of product component through crowdsourcing, novel ideas from outside the organization
2	Knowledge identification	**Important knowledge:** Knowledge about the specifications for the product component Knowledge about the core product, enough in order to fit the component to the core product **Holders of knowledge:** Product designers, crowdsourcing facilitators, crowdsourcing participants **Communication media:** Crowdsourcing platform
3	Threat identification	**Threat agent:** Competitors **Threat:** Exploitation of knowledge about new product development **Threat:** Exploitation of published crowdsourced plans despite copyright **Threat agent:** Crowdsourcing platform **Threat:** Loss of plans submitted to the platform **Threat agent:** Crowdsourcing contributors **Threat:** Exploitation of knowledge about the new product development **Threat:** Cause harm and extra work by contributing intentionally flawed designs
4	Risk analysis	**Exploitation of knowledge about new product development:** Potential medium impact, medium probability, medium size risk Loss of plans submitted to the platform: medium impact, low probability **Harm caused by flawed designs:** Low probability, medium impact **Reputation damage:** Low probability, low impact
5	Cost-benefit analysis	**Business benefits:** Faster innovation, faster time-to-market, more ideas for less resource spending. **Business costs:** Cost of crowdsourcing facilitator, time from designers to evaluate the results, time and effort to create specifications **Knowledge risks:** Leakage of knowledge to competitors **Knowledge risk mitigation costs:** Time to monitor the quality of submissions
6	Risk mitigation	**Mitigation:** Knowledge that is shared is limited only to the non-strategic component. Knowledge about the core product is not shared to the crowd. Crowdsourcing facilitator enforces the code of conduct in the crowdsourcing platform. Time is allocated for further design sprints immediately after the challenge to beat competitors
7	Monitoring	Crowdsourcing facilitator monitors discussions Crowdsourcing facilitator and **designers** monitor the incoming submissions and adjust the challenge rules and specifications accordingly

DISCUSSION

Knowledge and its creation are important sources of competitive advantage and business opportunities for most contemporary organizations (Alavi & Leidner, 2001; Choo, 1996; Grant, 1996; Nonaka & Takeuchi, 1995). Thus, knowledge risks have lately gained increasing attention in information security related literature (Jennex & Durcikova, 2014; Markus, Manhart & Thalmann, 2015; Olander, Hurmelinna-Laukkanen, & Vanhala, 2014). Also the recent developments

in social media use in organizations, as well as various open innovation practices that aim to make use of company-external information and knowledge in innovation, have raised new important challenges for knowledge security. Too large emphasis on threats instead of business benefits has led many companies to heavily limit or even deny the use of the above approaches, without careful consideration of business benefits. To address this topic, a systematic process model for business-driven management of knowledge security risks is proposed.

The KSRM approach differs in several respects from the few existing specifically knowledge- related risk management approaches. First, the identified existing knowledge security risk management models seem to focus strongly on merely the recognition and analysis of knowledge security risks. Some also help to identify the criticality of the various types of knowledge (Aljafari & Sarnikar, 2009; A.M. Padyab et al., 2014). However, the existing studies do not do this explicitly from the viewpoint of business needs and expected benefits, with the exception of the need to meet the requirements forced by laws, standards, customers, or internal regulations (cf. Thalmann et al., 2014). Second, even if some emphasize the importance of balancing the risk-related costs and benefits, they do not explicitly provide actual concrete approaches to do this or bring this important matter forth as a separate step in the risk management process. From the perspective of contemporary business in general, and especially from the perspective of e.g. relatively novel business approaches such as open innovation, crowdsourcing and social media that emphasize the open sharing of knowledge, it seems evident that all knowledge security risks cannot be eliminated or even controlled. This should not usually even be the priority of business-oriented knowledge security risk management. In this respect, a far more useful approach, due to the potentially huge business benefits received from adopting such business approaches, is trying to balance the benefits to risks and costs.

The illustrative example of a challenging community-based open innovation case demonstrates that risk management is clearly not anymore a technically-oriented task. It also demonstrates the importance of both business-orientation as well as the need for specifically knowledge- (not merely information) focused risk management process. It also demonstrates the need for involving various different organizational functions to knowledge risk analysis. The sensemaking nature of knowledge risk analysis, especially in the case of novel types of business approaches such as open innovation, crowdsourcing or social media- and community-based business practices, is demonstrated by the case. These activities often require the sharing of business-critical knowledge in discussions and other formats even outside the company boundaries. The use of traditional information security models, in this case, would have revealed e.g. the technical risks and probably would have strongly emphasized the threats of revealing product development- related information e.g. to competitors, instead of business-related benefits. Thus, there would be a high probability of IT managers to prohibit or limit the use of such approaches, despite their possibly significant potential for business and for the development of new business models.

Our model makes knowledge security risk management a business-driven process that balances the costs and benefits of knowledge sharing and protection. The model functions as a communication and sense-making tool for managers across organizational functions and boundaries. This approach is especially useful in situations where a company needs to consider business approaches that require opening up of information and knowledge in novel ways to company outsiders (customers, consumers, suppliers, communities, etc.), as well as when this information and knowledge might be searchable to competitors by novel means of business intelligence, such as data mining and social media analytics approaches.

CONCLUSION

With this paper the authors aimed to answer the research question "How can organizations manage knowledge risks in a business-driven way?" The paper argues that knowledge security risks should be managed as a systematic communication and sensemaking process, instead of risks and business benefits being traditionally evaluated in separate functions of companies. Different functions do not automatically communicate with each other in knowledge security issues, and need a framework in order to successfully do this. From this perspective, the authors have introduced a model that takes business needs into consideration in knowledge security management in several ways discussed above. The model contributes to current literature, because knowledge perspective is very seldom taken into consideration in information security literature, and the business perspective is not explicitly taken into consideration in extant knowledge security risk management models that were analyzed in this study.

REFERENCES

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

Alavi, M., & Leidner, D. E. (2001). Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues. *Management Information Systems Quarterly*, *25*(1), 107–136. doi:10.2307/3250961

Aljafari, R., & Sarnikar, S. (2009). A Framework for Assessing Knowledge Sharing Risks in Interorganizational Networks. *Proceedings AMCIS '09*. Retrieved from http://aisel.aisnet.org/amcis2009/572

Bandyopadhyay, K., Mykytyn, P. P., & Mykytyn, K. (1999). A framework for integrated risk management in information technology. *Management Decision*, *37*(5), 437–445. doi:10.1108/00251749910274216

Baskerville, R. (1991). Risk analysis as a source of professional knowledge. *Computers & Security*, *10*(8), 749–764. doi:10.1016/0167-4048(91)90094-T

Bolisani, E., & Scarso, E. (2014). The place of communities of practice in knowledge management studies: A critical review. *Journal of Knowledge Management*, *18*(2), 7–7. doi:10.1108/JKM-07-2013-0277

Braun, R., & Esswein, W. (2012). Corporate Risks in Social Networks–Towards a Risk Management Framework. *Proceedings of the Eighteenth Americas Conference on Information Systems*, Seattle. Retrieved from http://aisel.aisnet.org/amcis2012/proceedings/VirtualCommunities/9/

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing octave allegro: Improving the information security risk assessment process. *DTIC Document.* Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA470450

Choo, C. W. (1996). The knowing organization: How organizations use information to construct meaning, create knowledge and make decisions. *International Journal of Information Management*, *16*(5), 329–340. doi:10.1016/0268-4012(96)00020-5

Davenport, T. H., & Prusak, L. (1998). *Working Knowledge: How Organizations Manage What They Know*. Boston: Harvard Business School Press.

DeLoach, J. (2004). The new risk imperative–an enterprise-wide approach. Handbook of Business Strategy, 5(1), 29–34.

Desouza, K. C. (2006). Knowledge Security: An Interesting Research Space. *Journal of Information Science & Technology*, *3*(1). Retrieved from http://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=15450287&AN=25759169&h=6LMP09JhpDAlfN39B%2FP7ajMwinQ6nx%2FAj1Ojmu11ST58%2B3Ch%2F1N4SKZIP2%2F6qrf6aW07ULFqd1XvhUdGyFDGOA%3D%3D&crl=c

Desouza, K. C., & Vanapalli, G. K. (2005). Securing knowledge in organizations: Lessons from the defense and intelligence sectors. *International Journal of Information Management*, *25*(1), 85–98. doi:10.1016/j.ijinfomgt.2004.10.007

Easterby-Smith, M., Lyles, M. A., & Tsang, E. W. (2008). Inter-organizational knowledge transfer: Current themes and future prospects. *Journal of Management Studies*, *45*(4), 677–690. doi:10.1111/j.1467-6486.2008.00773.x

Farahmand, F., Navathe, S. B., Enslow, P. H., & Sharp, G. P. (2003). Managing Vulnerabilities of Information Systems to Security Incidents. *Proceedings of the 5th International Conference on Electronic Commerce* (pp. 348–354). New York, NY, USA: ACM. http://doi.org/ doi:10.1145/948005.948050

Grant, R. M. (1996). Toward a knowledge-based theory of the firm. *Strategic Management Journal*, *17*(S2), 109–122. doi:10.1002/smj.4250171110

Haefliger, S., Monteiro, E., Foray, D., & von Krogh, G. (2011). Social software and strategy. *Long Range Planning*, *44*(5), 297–316. doi:10.1016/j.lrp.2011.08.001

Hansen, M. T. (1999). The Search-Transfer Problem: The Role of Weak Ties in Sharing Knowledge across Organization Subunits. *Administrative Science Quarterly*, *44*(1), 82–111. doi:10.2307/2667032

Ilvonen, I. (2013). Knowledge Security-A Conceptual Analysis. *Tampereen Teknillinen Yliopisto. Julkaisu-Tampere University of Technology. Publication 1175*. Retrieved from https://dspace.cc.tut.fi/dpub/handle/123456789/21835

Jafari, M., Rezaeenour, J., Mazdeh, M. M., & Hooshmandi, A. (2011). Development and evaluation of a knowledge risk management model for project-based organizations: A multi-stage study. *Management Decision*, *49*(3), 309–329. doi:10.1108/00251741111120725

Jennex, M. (2014). A proposed method for assessing knowledge loss risk with departing personnel. *Vine*, *44*(2), 185–209. doi:10.1108/VINE-07-2012-0028

Jennex, M., & Durcikova, A. (2014). Integrating IS Security with Knowledge Management: Are We Doing Enough? *International Journal of Knowledge Management*, *10*(2), 1–12. doi:10.4018/ijkm.2014040101

Jennex, M. E., & Zyngier, S. (2007). Security as a contributor to knowledge management success. *Information Systems Frontiers*, *9*(5), 493–504. doi:10.1007/s10796-007-9053-4

Kogut, B., & Zander, U. (1992). Knowledge of the firm, combinative capabilities, and the replication of technology. *Organization Science*, *3*(3), 383–397. doi:10.1287/orsc.3.3.383

Lichtenstein, S. (1996). Factors in the selection of a risk assessment method. *Information Management & Computer Security*, *4*(4), 20–25. doi:10.1108/09685229610130503

Manhart, M., & Thalmann, S. (2013). An Integrated Risk Management Framework: Measuring the Success of Organizational Knowledge Protection. Retrieved from http://aisel.aisnet.org/amcis2013/BusinessIntelligence/RoundTablePresentations/7/

Manhart, M., & Thalmann, S. (2015). Protecting organizational knowledge: A structured literature review. *Journal of Knowledge Management*, *19*(2), 190–211. doi:10.1108/JKM-05-2014-0198

Marabelli, M., & Newell, S. (2012). Knowledge risks in organizational networks: The practice perspective. *The Journal of Strategic Information Systems*, *21*(1), 18–30. doi:10.1016/j.jsis.2011.11.002

Matayong, S., & Mahmood, A. K. (2013). The review of approaches to knowledge management system studies. *Journal of Knowledge Management*, *17*(3), 472–490. doi:10.1108/JKM-10-2012-0316

Nonaka, I., & Takeuchi, H. (1995). The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation: How Japanese Companies Create the Dynamics of Innovation. New York: Oxford University Press. Retrieved from http://www.google.com/books?hl=fi&lr=&id=B-qxrPaU1-MC&oi=fnd&pg=PA3&dq=nonaka+knowledge+creating+company&ots=XgZMnwsihY&sig=uZcw6er74CSraZHdULf_2R8-fKw

O'Donoghue, N., & Croasdell, D. T. (2009). Protecting knowledge assets in multinational enterprises: A comparative case approach. *Vine*, *39*(4), 298–318. doi:10.1108/03055720911013616

Olander, H., Hurmelinna-Laukkanen, P., & Vanhala, M. (2014). Mission: Possible but sensitive — knowledge protection mechanisms serving different purposes. *International Journal of Innovation Management*, *18*(06), 1440012. doi:10.1142/S136391961440012X

Olander, H., Vanhala, M., & Hurmelinna-Laukkanen, P. (2014). Reasons for choosing mechanisms to protect knowledge and innovations null. *Management Decision*, *52*(2), 207–229. doi:10.1108/MD-11-2012-0791

Padyab, A. M., Päivärinta, T., & Harnesk, D. (2014). Genre-Based Approach to Assessing Information and Knowledge Security Risks. *International Journal of Knowledge Management*, *10*(2), 13–27. doi:10.4018/ijkm.2014040102

Padyab, A. M., Paivarinta, T., & Harnesk, D. (2014). Genre-Based Assessment of Information and Knowledge Security Risks. *Proceedings of the 2014 47th Hawaii International Conference on System Sciences (HICSS)* (pp. 3442–3451). http://doi.org/ doi:10.1109/HICSS.2014.428

Peltier, T., Peltier, J., & Blackley, J. (2005). *Information Security Fundamentals*. Boca Raton: CRC Press.

Randeree, E. (2006). Knowledge management: Securing the future. *Journal of Knowledge Management*, *10*(4), 145–156. doi:10.1108/13673270610679435

Ryan, J. J. (2006). Managing knowledge security. *Vine*, *36*(2), 143–145. doi:10.1108/03055720610682942

Shedden, P., Scheepers, R., Smith, W., & Ahmad, A. (2011). Incorporating a knowledge perspective into security risk assessments. *Vine*, *41*(2), 152–166. doi:10.1108/03055721111134790

Shedden, P., Smith, W., & Ahmad, A. (2010). Information Security Risk Assessment: Towards a Business Practice Perspective. *Australian Information Security Management Conference*. Retrieved from http://ro.ecu.edu.au/ism/98

Siponen, M. T. (2000). Critical analysis of different approaches to minimizing user-related faults in information systems security: Implications for research and practice. *Information Management & Computer Security*, *8*(5), 197–209. doi:10.1108/09685220010353178

Siponen, M. T. (2005). Analysis of modern IS security development approaches: Towards the next generation of social and adaptable ISS methods. *Information and Organization*, *15*(4), 339–375. doi:10.1016/j.infoandorg.2004.11.001

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A Review of Information Security Issues and Respective Research Contributions. *SIGMIS Database*, *38*(1), 60–80. doi:10.1145/1216218.1216224

Spears, J. L. (2006). A holistic risk analysis method for identifying information security risks. In *Security Management, Integrity, and Internal Control in Information Systems* (pp. 185–202). Springer. Retrieved from http://link.springer.com/chapter/10.1007/0-387-31167-X_12

Spender, J.-C., & Grant, R. M. (1996). Knowledge and the firm: Overview. *Strategic Management Journal*, *17*(S2), 5–9. doi:10.1002/smj.4250171103

Spremic, M. (2012). Corporate IT Risk Management model: A holistic view at managing information system security risks. *Proceedings of the ITI 2012 34th International Conference on Information Technology Interfaces (ITI)* (pp. 299–304). IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6308022

Spruit, M. E., & Looijen, M. (1996). IT security in Dutch practice. *Computers & Security*, *15*(2), 157–170. doi:10.1016/0167-4048(96)00001-6

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. *Nist Special Publication*, *800*(30), 800–830.

Szulanski, G. (2000). The process of knowledge transfer: A diachronic analysis of stickiness. *Organizational Behavior and Human Decision Processes*, *82*(1), 9–27. doi:10.1006/obhd.2000.2884

Thalmann, S., Manhart, M., Ceravolo, P., & Azzini, A. (2014). An Integrated Risk Management Framework: Measuring the Success of Organizational Knowledge Protection. *International Journal of Knowledge Management*, *10*(2), 28–42. doi:10.4018/ijkm.2014040103

Thierauf, R. J. (2001). *Effective business intelligence systems*. Greenwood Publishing Group. Retrieved from http://www.google.com/books?hl=fi&lr=&id=miXiZGYEpj8C&oi=fnd&pg=PR7&dq=Effective+Business+Intelligence+Systems&ots=-gRg90lO1b&sig=k5jswIfojp9xni9vENWH3GvYRYg

Trkman, P., & Desouza, K. C. (2012). Knowledge risks in organizational networks: An exploratory framework. *The Journal of Strategic Information Systems*, *21*(1), 1–17. doi:10.1016/j.jsis.2011.11.001

Tzortzaki, A. M., & Mihiotis, A. (2014). A Review of Knowledge Management Theory and Future Directions. *Knowledge and Process Management*, *21*(1), 29–41. doi:10.1002/kpm.1429

Varnell-Sarjeant, J. F. (2008). Managing a Man-rated Software Development Program via Risk Mitigation. *SIGSOFT Softw. Eng. Notes, 33*(4), 8:1–8:8. doi:10.1145/1384139.1384147

Väyrynen, K., Hekkala, R., & Liias, T. (2013). Knowledge Protection Challenges of Social Media Encountered by Organizations. *Journal of Organizational Computing and Electronic Commerce*, *23*(1-2), 34–55. doi:10.1080/10919392.2013.748607

von Krogh, G. (2009). Individualist and collectivist perspectives on knowledge in organizations: Implications for information systems research. *The Journal of Strategic Information Systems*, *18*(3), 119–129. doi:10.1016/j.jsis.2009.08.001

von Krogh, G. (2012). How does social software change knowledge management? Toward a strategic research agenda. *The Journal of Strategic Information Systems*, *21*(2), 154–164. doi:10.1016/j.jsis.2012.04.003

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, *23*(5), 371–376. doi:10.1016/j.cose.2004.05.002

Ward, J., & Daniel, E. (2006). *Benefits management: delivering value from IS and IT investments*. John Wiley & Sons. Retrieved from http://www.google.com/books?hl=fi&lr=&id=gUfOADrebgIC&oi=fnd&pg=PR2&dq=ward+benefits+management&ots=a3Mms7An8f&sig=_Qi2m948YeP8g1nPOK9_MmTAQhc

Webb, J., Maynard, S., Ahmad, A., & Shanks, G. (2013). Towards an Intelligence-Driven Information Security Risk Management Process for Organisations. *Presented at the 24th Australasian Conference on Information Systems: Intelligence-Driven ISRM for Organisations*, Melbourne. Retrieved from http://people.eng.unimelb.edu.au/seanbm/research/2013ACISWebb.pdf

Whitman, M., & Mattord, H. (2011). *Principles of information security*. Cengage Learning. Retrieved from http://www.google.com/books?hl=fi&lr=&id=L3LtJAxcsmMC&oi=fnd&pg=PR9&dq=+Principles+of+Information+Security&ots=6UK6WReSwQ&sig=j0Mz7Xm1qZRdzj33K-bc-j02les

Ilona Ilvonen is a post-doctoral researcher and university teacher at the department of Information Management and Logistics in Tampere University of Technology. Her research interests are in knowledge security or protection and knowledge sharing in organizations, and especially the balancing act required between these two activities. She has published several articles on the topic since the year 2006.

Jari Jussila, DSc (Tech.), is working at Tampere University of Technology, Novi Research Center as Postdoctoral Researcher. He completed his Doctoral thesis on social media use in business-to-business companies' innovation. His research is currently focused on social media, communities, crowdsourcing, as well as, big social data analytics.

Dr. Hannu Kärkkäinen is Professor of Knowledge Management at the Department of Information Management and Logistics at Tampere University of Technology in Finland. His current research interests include social media in business, knowledge management and decision making in innovation, organizational learning, customer needs assessment in business-to-business organizations, and the co-operation and value networks in innovation. He has published a number of refereed international journal articles in journals like International Journal of Technology Management, R&D Management *and* International Journal of Production Economics*, as well as books and other publications on the above research topics.*