Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2015 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-13-2015

Business orientation in knowledge security risk management – a literature review

Ilona Ilvonen
Tampere University of Technology

Jari Jussila
Tampere University of Technology

Business orientation in knowledge security risk management – a literature review

Research paper

Ilona Ilvonen
Tampere University of Technology, Tampere, Finland {ilona.ilvonen@tut.fi}

Jari Jussila
Tampere University of Technology, Tampere, Finland {jari.j.jussila@tut.fi}

ABSTRACT

This paper examines the information systems literature field from the viewpoint of knowledge security risk management. The review this paper reports was able to identify 7 papers presenting a knowledge security risk management model. The models represent different takes and perspectives on knowledge security risk management. The main finding is that business orientation in the risk management models, and a comprehensive approach that would emphasize also continuous monitoring of the implementation and success of the risk mitigation solutions are not common in the literature. We suggest further theoretical and empirical studies that would address these issues.

Keywords: Knowledge security risk, risk management model, knowledge risk, literature review

INTRODUCTION

Knowledge and its creation are important sources of competitive advantage and business opportunities for most contemporary organizations (Alavi and Leidner 2001; Choo 1996; Grant 1996; Nonaka and Takeuchi 1995). Although knowledge creation and knowledge management have been researched extensively (e.g. Matayong and Mahmood 2013; Tzortzaki and Mihiotis

2014), there is one viewpoint to knowledge that has received less attention: knowledge security risk management (Shedden et al. 2011). Most existing risk analysis methods can be regarded as providing a plain technical view on information and technological assets (e.g. Ahmad et al. 2014; Padyab et al. 2014; Shedden et al. 2010; Spears 2006), ignoring that knowledge is bound to people and as a consequence people and especially their communication are significant sources of knowledge security risks (e.g. Ilvonen 2013; Jarvenpaa and Majchrzak 2015; Padyab et al. 2014). Knowledge security risk in this paper is defined as a risk of leaking or losing important knowledge that contributes to the competitiveness of an organization.

Ahmad et al. (2014) note several studies that point out that increasing the circulation of knowledge also increases the risk of leakage (Desouza 2006; Desouza and Vanapalli 2005; Easterby-Smith et al. 2008; Trkman and Desouza 2012). New forms of organizational operation, such as open innovation, as well as various organizational approaches of social media, emphasize opening up of organizational knowledge resources towards customers and other organizational stakeholders. Organizations need also more efficient ways to collect knowledge originating from outside the boundaries of the organization. The risks this opening causes should be adequately addressed in connection with the business benefits that are sought by more openly sharing knowledge. Literature addressing these issues seems to be scarce, and this review is conducted to gain an understanding of what has been published under the topic of knowledge security risk management.

This paper answers to the question: How do knowledge security risk management models, if there are any, address the connection to business goals? The assumption behind this research is, that there are not many risk management models that would address the security and protection of knowledge specifically, and those models that do exist, would not be business

oriented. Next we present the research methodology we followed, along with the results. At the end of the paper we discuss the implications of our findings for both research and practice.

RESEARCH APPROACH AND METHODOLOGY

In this paper we present a literature review (Tranfield et al. 2003) on knowledge security risk management. For example, a search for "knowledge security risk" in several scientific article databases (AIS electronic library, ACM digital library, IEEE Xplore, and Emerald) there are only a few search results. In order to find knowledge risk management models beyond the actual term, we conducted several keyword searches ("knowledge security risk management", "risk management model", "knowledge risk", "knowledge risk management framework", "risk management framework") into these databases. In total our searches found 695 articles. We believe these articles are a good representation of the current literature on the topic. Although we did not use time constraints in our searches, the topic is relatively new, so most of the search results were from the past 10 to 15 years.

The 695 articles were screened through based on title, and abstract if needed, by two researchers independently. For the full paper review we selected papers that potentially considered knowledge risks in the information systems domain and the management of these risks in some way, were available to us in full paper, and were written in English. The papers that were excluded either did not discuss risk management at all, or considered the management of financial risks, which was considered outside the scope of this study (Lawsirirat and Gupta 2008).

There were several articles that were excluded by one researcher and included by another, and all of these papers were included in the full paper review to ensure that relevant literature is not overlooked. Total of 33 papers were included in the full paper review, in which we screened

the papers if they present a risk management model that addresses knowledge risks. The full papers were read and classified by two researchers independently, after which there was a discussion of what papers would be included in the final review. Most papers excluded at this stage presented project risk management models that discussed project-relevant knowledge, but not how the knowledge risks in the project should be managed, such as (Smith et al. 2005).

KNOWLEDGE RISK MANAGEMENT MODELS

The review was able to identify altogether 7 articles that discussed various types of processes and frameworks in the specific field of knowledge risk management. The foci of the articles are presented in Table 1.

Table 1. Summary of the literature review findings

Article	Viewpoint on knowledge security risk management	Knowledge security risk management process model phases	Model's support on business perspective
Ilvonen et al. (2015)	Framework for managing knowledge security risks	Identify business need, identify important knowledge, identify threats to knowledge, analyse risks, conduct cost/benefit analysis, implement mitigation measures, monitor	Business perspective identified as essential
Padyab et al. (2014)	Implementing genre-based assessment of information and knowledge security risks	Define stakeholders of security risk analysis, Define risk measurement criteria, Identify producers and users of information, Identify genres of communication, Develop an information asset profile with genre properties, Identify containers, Identify risks and mitigation strategies	Business perspective not explicitly elaborated, but supports focusing on stakeholders that are perceived important according to organizational strategic goals and objectives
Manhart & Thalmann (2013)	Risk management framework for measuring the success of organizational knowledge protection	Select control objectives, Design of controls, Verify control implementations	Business perspective based on need to meet requirements forced by laws, standards, customers or internal regulations

Trkman & Desouza (2012)	Classification framework of knowledge risks and the development of a common language for knowledge risk management	Framework for identifying, classifying and mitigating knowledge risks; does not present knowledge security risk management as a process	Business perspective not explicitly elaborated, supports reducing transaction costs in inter-organizational collaboration by making explicit both risks and knowledge transfer benefits
Shedden et al. (2011)	Incorporating a knowledge perspective into information security risk assessments	Asset identification (people), critical knowledge identification (held by individuals and communities, risk mitigation (via traditional IS risk mitigation and SECI process)	Business perspective not explicitly elaborated, but supports focusing on processes critical for business
Shedden et al. (2010)	Incorporation of a business practice perspective to ISRA methods supporting the identification of important process knowledge of organizations	Identification of information and knowledge assets, vulnerability and risk identification	Business perspective not explicitly elaborated, but supports focusing on processes critical for business
Aljafari & Sarnikar (2009)	Identification of valuable knowledge assets potentially exposed through the use of collaboration technologies in inter-organizational networks	Identify knowledge assets, Identify inter-organizational knowledge sharing practice, Identify collaboration technology, Identify vulnerabilities and threats to knowledge assets, Make assertions, Provide evidence, Calculate risks, Develop policy	Supports focusing on involving business managers in the knowledge risk management process and helping to identify strategic knowledge assets which are critical to business

Since the process model presented by Ilvonen et al. (2015) seemed to cover the phases of risk management most broadly, we have structured the following review according to the steps of their model.

Business orientation

Most of the existing knowledge risk management models only superficially discuss their perspective towards business and the actual business triggers (business need, business problem, expected benefits) that should start the knowledge risk management process. Only Ilvonen et al. (2015) emphasize the importance of business orientation of knowledge risk management. The few links to business that the other models do provide include: guiding focus on processes

critical for business (Shedden et al. 2010, 2011), guiding focus on stakeholders who are perceived important according to organizational strategic goals and objectives (Padyab et al. 2014), helping to identify 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 and Sarnikar 2009), supporting reduction of transaction costs in inter-organizational collaboration by making explicit both risks and knowledge transfer benefits (Trkman and Desouza 2012), and ensuring that knowledge protection meet requirements forced by laws, standards, customers or internal regulations (Manhart and Thalmann 2013).

Knowledge identification

Six of the papers (Aljafari and Sarnikar 2009; Ilvonen et al. 2015; Padyab et al. 2014; Shedden et al. 2010, 2011; Trkman and Desouza 2012) emphasize the importance of identifying knowledge assets in the knowledge risk management process. In addition, the authors provide the following approaches and tools in assisting the identification of knowledge assets: Knowledge reservoirs graph designed by Becerra-Fernandez, Gonzalez, and Shabherwal (2004); Knowledge Capability Areas (KCA) proposed by Freeze and Kulkarni (2005), and VRIN framework Barney (1991, 1996) for identifying strategic knowledge assets by assessing their (1) value, (2) rareness, (3) imitability, (4) non-substitutability, in locating knowledge assets (Aljafari and Sarnikar 2009); conducting qualitative interviews with relevant staff members in the context of key business processes (Shedden et al. 2011); and the hybrid Genre Based Method (GBM) and OCTAVE Allegro (OA) method in identifying critical information and knowledge assets (Padyab et al. 2014).

Threat identification

Most of the models (Aljafari and Sarnikar 2009; Ilvonen et al. 2015; Padyab et al. 2014; Shedden et al. 2011; Trkman and Desouza 2012) include threat identification as an essential process phase, either as an individual process phase, or as a part of the risk analysis phase in the knowledge risk management process. However, only one of the discovered models included a method and a tool for identifying threats related to knowledge assets: the Octave Allegro method and it's worksheets (Padyab et al. 2014).

Risk analysis

Several of the models discuss risk analysis (Aljafari and Sarnikar 2009; Ilvonen et al. 2015; Padyab et al. 2014; Trkman and Desouza 2012) as a process phase in knowledge risk management. Aljafari & Sarnikar (2009) include sub-phases of making assertions, providing evidence to support assertions, 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).

Risk mitigation

Risk mitigation is addressed in several of the studied models (Aljafari and Sarnikar 2009; Ilvonen et al. 2015; Manhart and Thalmann 2013; Padyab et al. 2014; Shedden et al. 2011). Aljafari & Sarnikar (2009) propose developing security policies as the primary means of

mitigating risks. Shedden et al. (2011) propose the SECI model (Nonaka and Takeuchi 1995) of socialization, externalization, combination and internalization as a way to mitigate knowledge risks (Shedden et al. 2011). Manhart & Thalmann (2013) suggest internal knowledge audits as means of risk mitigation by auditing the performance metrics of knowledge protection controls. Ilvonen et al. (2015) propose training in many cases as the main knowledge risk mitigation measure.

Cost-benefit analysis

Cost-benefit analysis received little attention in the knowledge risk management models. Manhart & Thalmann (2013) address the cost-benefit analysis in terms of risk mitigation, from the perspective of assessing the performance of knowledge protection but not for evaluating or balancing the costs and benefits of knowledge sharing and knowledge protection. Also Padyab et al. (2014) argue that the output from risk assessment will help organizations to conduct a cost-benefit analysis based on current controls and countermeasures to whether mitigate, transfer, avoid or accept the risks, but do not consider balancing the costs (of mitigation) with business benefits. Ilvonen et al. (2015) emphasize cost-benefit analysis not only in light of the mitigation costs, but also in light of the entire business costs and benefits to better balance the costs and benefits of knowledge risk management.

Monitoring

Also risk monitoring received little attention in the knowledge security risk management models. Manhart & Thalmann (2013) propose monitoring knowledge security by means of knowledge audits. Ilvonen et al. (2015) suggest constant monitoring for changes in environment, knowledge or threats, and a re-assessment of knowledge risks when appropriate.

DISCUSSION AND CONCLUSIONS

The first part of the research question, whether knowledge risk management models are found in contemporary literature, is answered clearly with the previous section of this paper. There are theoretical models that address the security and protection of knowledge assets, and some of them do consider the business needs and identification of valuable knowledge, that we stressed as being very important to businesses in the introduction of this paper. However, the development of these models is still in the early stages, and there is need for empirical research on the field.

The literature that our review was able to locate comes mainly from conferences, which indicates that the topic of knowledge security risk management is young, and has not made its way to higher quality journal publications. We decided to include also conference articles in our full paper review, since limiting the search to only journals would have excluded a large section of our results. The conference papers, however, indicate that studies in this field are ongoing and the results of a similar review in a few years will turn out different kinds of results. The increasing importance of knowledge for most businesses, and the continuously evolving digital environment will keep knowledge security on the radar of managers well into the future.

The identified existing knowledge security risk management models seem to focus on the recognition and analysis of knowledge security risks. Some also point out that identifying critical knowledge is an important step in the process (Aljafari and Sarnikar 2009; Padyab et al. 2014). Only Ilvonen et al. (2015) suggest this to be done explicitly from the viewpoint of business needs, problems and expected benefits. Another perspective to business orientation was to meet the requirements forced by laws, standards, customers, or internal regulations (cf. Manhart & Thalmann 2013). We argue that a stronger standpoint of business need identification would

involve both the business managers as well as the security managers (e.g. chief information security officer) of an organization to the risk management process from early on. The business perspective should be more clearly emphasized in all risk management models to make the practical implementation of the model reasonable and avoid using resources to tackle non-relevant risks.

One thing that stands out from the reviewed papers is that they are theoretical developments, and have not yet been extensively empirically tested. Two of the papers (Ilvonen et al. 2015; Shedden et al. 2011) report some empirical testing of the models, but these are more of the nature of initial validation than robust testing. This indicates that the research on knowledge security risk management is still in its early stages, and further empirical studies on the field are needed to complement the ones that might be on the way at the moment. Testing the knowledge security risk management models well would require for example action design research approach, and both quantitative and qualitative research methods to be used in order to gather evidence of the impact of the model to business as well as the experiences of the managers that are using it. Especially interesting would be longitudinal case studies that would be able to identify longer term benefits of applying a business oriented knowledge risk management model.

As every study, we acknowledge that also this study has its limitations. The review reported in this paper does not comprehensively cover all information systems research outlets, but still covers a good representation of them, while also offering a view to the knowledge management research outlets. Also reviewing only articles that present a knowledge risk management process model gives a limited view on all the literature that is related to knowledge security risks. This review adequately answers to the research question we posed, but we identify

a need for theoretical research that would examine knowledge risk management also from broader perspectives. This review identifies a lack of emphasize on the later steps of the risk management models, i.e. the risk mitigation and monitoring steps. Theoretical research that would drill into the "how" this is done would perhaps bring out literature that addresses these stages more than the literature analyzed in this study. This theoretical research could then be followed by empirical research to gather experiences of how the identified practices work in organizations.

Since there is no unified definition to knowledge risk management, identifying all the relevant literature is challenging. Augmenting the searches to more databases and a broader set of search concepts would have generated more search results. The authors feel that these results would not have been substantially different in the specific aim of finding a knowledge risk management model or framework, while they would have expanded the review beyond the resources that were available for this study.

REFERENCES

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

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

Aljafari, R., and Sarnikar, S. 2009. "A Framework for Assessing Knowledge Sharing Risks in Interorganizational Networks," *AMCIS 2009 Proceedings* (available at http://aisel.aisnet.org/amcis2009/572).

Barney, J. 1991. "Firm Resources and Sustained Competitive Advantage," *Journal of Management* (17:1), p. 99.

Barney, J. B. 1996. "The resource-based theory of the firm," *Organization science* (7), pp. 469–469.

Becerra-Fernandez, I., Gonzales, A., and Shabherwal, R. 2004. *Knowledge Management and KM Software Packages*, Prentice Hall.

Bolisani, E., and Scarso, E. 2014. "The place of communities of practice in knowledge management studies: a critical review," *Journal of Knowledge Management* (18:2), pp. 7–7.

Caralli, R. A., Stevens, J. F., Young, L. R., and Wilson, W. R. 2007. "Introducing octave allegro: Improving the information security risk assessment process," DTIC Document (available at 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), pp. 329–340 (doi: 10.1016/0268-4012(96)00020-5).

Dempster, A. P. 1967. "A generalization of Bayesian inference," DTIC Document (available at http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=AD0664659).

Desouza, K. C. 2006. "Knowledge Security: An Interesting Research Space.," *Journal of Information Science & Technology* (3:1) (available at 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., and Vanapalli, G. K. 2005. "Securing knowledge in organizations: lessons from the defense and intelligence sectors," *International Journal of Information Management* (25:1), pp. 85–98.

Easterby-Smith, M., Lyles, M. A., and Tsang, E. W. 2008. "Inter-organizational knowledge transfer: Current themes and future prospects," *Journal of management studies* (45:4), pp. 677–690.

Freeze, R., and Kulkarni, U. 2005. "Knowledge Management Capability Assessment: Validating a Knowledge Assets Measurement Instrument," in *Proceedings of the 38th Annual Hawaii International Conference on System Sciences, 2005. HICSS '05*, Presented at the Proceedings of the 38th Annual Hawaii International Conference on System Sciences, 2005. HICSS '05, , January, p. 251a–251a (doi: 10.1109/HICSS.2005.375).

Grant, R. M. 1996. "Toward a knowledge-based theory of the firm," *Strategic management journal* (17), pp. 109–122.

Ilvonen, I. 2013. "Knowledge Security-A Conceptual Analysis," *Tampereen teknillinen yliopisto. Julkaisu-Tampere University of Technology. Publication; 1175* (available at https://dspace.cc.tut.fi/dpub/handle/123456789/21835).

Ilvonen, I., Jussila, J., Karkkainen, H., and Paivarinta, T. 2015. "Knowledge Security Risk Management in Contemporary Companies – Toward a Proactive Approach," in *2015 48th Hawaii International Conference on System Sciences (HICSS)*, Presented at the 2015 48th Hawaii International Conference on System Sciences (HICSS), , January, pp. 3941–3950 (doi: 10.1109/HICSS.2015.472).

Jarvenpaa, S., and Majchrzak, A. 2015. "Interactive Self-Regulatory Theory for Sharing and Protecting in Inter-Organizational Collaborations," *Academy of Management Review*, p. amr.2012.0005 (doi: 10.5465/amr.2012.0005).

Lawsirirat, C., and Gupta, A. 2008. "Creating Financial Risk Management Framework for the Service Delivery of Long-Term Service Agreements," *Proceedings of the 4th IEEE*

International Conference on Management of Innovation and Technology, ICMIT (doi: 10.1109/ICMIT.2008.4654536).

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

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

Nonaka, I., and 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 (available at 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).

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

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

Shafer, G. 1976. *A mathematical theory of evidence* (Vol. 1), Princeton university press Princeton (available at http://www.glennshafer.com/books/amte.html).

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

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

Smith, J., Bohner, S., and McCrickard, D. 2005. "Project management for the 21st century: supporting collabrative design through risk analysis," in *Proceedings of the 43rd annual Southeast regional conference - Volume 2*, Presented at the ACM-SE 43, ACM.

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

Tranfield, D., Denyer, D., and Smart, P. 2003. "Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review," *British Journal of Management* (14:3), pp. 207–222 (doi: 10.1111/1467-8551.00375).

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

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

Acknowlegdements: This research was funded by Academy of Finland grant #259831