Enforcing Organizational Knowledge Protection: An Investigation of Currently Applied Measures

Stefan Thalmann  
Innsbruck University School of Management University of Innsbruck Innsbruck Austria, stefan.thalmann@uibk.ac.at

Markus Manhart  
University of Innsbruck, School of Management, markus.manhart@uibk.ac.at

Follow this and additional works at: http://aisel.aisnet.org/wisp2012

Recommended Citation
http://aisel.aisnet.org/wisp2012/34

This material is brought to you by the Pre-ICIS Workshop on Information Security and Privacy (SIGSEC) at AIS Electronic Library (AISeL). It has been accepted for inclusion in WISP 2012 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Enforcing Organizational Knowledge Protection: An Investigation of Currently Applied Measures

Stefan Thalmann\textsuperscript{1}  
University of Innsbruck, School of Management, Innsbruck, Austria

Markus Manhart\textsuperscript{2}  
University of Innsbruck, School of Management, Innsbruck, Austria

\textbf{ABSTRACT}

Nowadays, organizations increasingly pay attention to protecting their data and information but at the same time the protection of their knowledge is neglected or underdeveloped in many cases. To maintain an organization’s competitive advantage, organisational risk management should pay more attention to the protection of knowledge. Scholarly knowledge management literature mainly concentrated on the facilitation of knowledge sharing and widely neglected this topic so far. In this paper we present results of a knowledge café that we ran with 18 IT professionals to investigate the current state of knowledge protection practice. It turned out that some organizational measures are applied in a rather uncoordinated manner, that only few technical measures are applied. Further, the performance measurement of knowledge protection lacks behind.

\textbf{Keywords:} Knowledge protection, Risk management framework, Protection measures, Knowledge café.

\textsuperscript{1}Corresponding author: stefan.thalmann@uibk.ac.at.

\textsuperscript{2}Corresponding author: markus.manhart@uibk.ac.at.
INTRODUCTION

It is no secret that organizations heavily rely on information systems (IS) nowadays, paying increasingly attention to protecting them as consequences of security breaches are heavy (Dhillon et al. 2006). Recently, companies take on great efforts to protect their data, spending a lot of money and resources to implement organizational frameworks such as COBIT and also engage with auditors to verify these implementations (Thalmann et al. 2012). At the same time, although knowledge is considered as an important organizational asset, knowledge managers seem to pay little attention to security issues (Asllani et al. 2003). Rather, knowledge protection is frequently considered to be a barrier to knowledge sharing from a knowledge management perspective (Khamseh et al. 2008) although empirical research shows that successful knowledge protection significantly enhances organizational performance (Mills et al. 2011).

Neglecting knowledge protection can reduce competitive advantage or cause replication of ideas by external organizations. Hence, finding a balance between protecting and sharing knowledge is crucial to solve the boundary paradox (Norman 2002). The challenge of finding this balance is even exacerbated by recent developments in the field of social media and mobile technologies that seem on the one hand promising to support organizations in their knowledge sharing (Santos et al. 2012) but on the other hand, this creates challenges to protect knowledge especially as it blurs the borders between work and leisure time (Väyrynen et al. 2013). Hence, firms need to preserve necessary information flows with partners but also have to decide upon what parts of knowledge to protect as well as how to enforce that (Norman 2002), which clearly demands an overall knowledge protection strategy (Olander et al. 2011). However, many organisations seem to lack a clear knowledge-protection strategy that tackles knowledge protection in a systematic way (Olander et al. 2011). To overcome these challenges, we proposed
an integrated risk management framework in prior research, taking the data as well as the knowledge perspective into account (Manhart et al. 2013). Based on this framework, we investigated the following research question with 18 practitioners: Which measures are currently used for protecting organisational knowledge?

**RELATED WORK**

In the domain of IS, a distinction between data, information and knowledge is widespread (Alavi et al. 2001). Data are the raw and unanalysed elements consisting of symbols and are input to an interpretation process. Information is related to meaning and thus results from the aggregation of data by means of logical, statistical or mathematical processing. Knowledge is characterized through the relation to the user, his interpretation, the application and thus on the impact on the user (Maier 2007).

Knowledge protection, as one of the three central organizational knowledge management strategies amongst knowledge creation and knowledge transfer (Bloodgood et al. 2001), is a firm’s efforts to prevent knowledge “from being altered, transferred to other organizations, lost, or becoming obsolete” (Bloodgood et al. 2001). Whilst the enforcement of data and information security is very structured and rigidly performed (cf. Arsan et al. 2013; Sillaber et al. 2013) and also checked (Bachlechner et al. 2014) by organizations recently, knowledge protection has been widely neglected in literature and practice so far (Väyrynen et al. 2013). Documented organizational knowledge which is stored in the organizational knowledge base is similar to information assets (Desouza 2006) and can be protected with information security measures, which have been discussed widely (Desouza et al. 2005; Trkman et al. 2012). They, however, do not apply fully to explicit knowledge which is not stored in officially endorsed documents. Even
more difficult is tacit knowledge which is sticky and complex and is not visible when observed (Nonaka et al. 1995). Both unclassified explicit knowledge as well as tacit knowledge are communicated via information channels but their detection is challenging, which makes many protection methods inappropriate (Liebeskind 1996) (see Figure 1).

![Figure 1. Protection of Tacit and Explicit Knowledge.](image)

Even if knowledge protection is of great importance, to the best of our knowledge, no overarching frameworks for knowledge protection exist. Therefore we proposed the integrated risk management framework in prior research (Manhart et al. 2013) depicted in Figure 2. In our view, organizational risk management is the overarching driver for IT security management as well as for knowledge protection. The goals defined by risk management are currently implemented by means of IT security measures for data and information (cf. Arsac et al. 2013) and should be implemented by knowledge protection measures for knowledge. However, knowledge protection lacks systematic approaches, i.e. an overall strategy for this implementation, nowadays (Olander et al. 2011). Hence, we propose that well known and established concepts and practices from IT security management should be adapted to the domain of knowledge protection. Implementing controls for knowledge protection also provides
benefits to organizations in terms of performance measurement. Linking high-level risk requirements with concrete mechanisms allows organizations to measure performance. Further, the implementation of controls for knowledge protection also allows organizations to conduct meaningful audits (Manhart et al. 2013).

![Risk Management Diagram]

**Figure 2.** An integrated risk management framework (Manhart et al. 2013).

**PROCEDURE**

The goal of this study is to investigate the current state of practice in regard to knowledge protection. Therefore, we ran a knowledge café, a kind of focus group interview, with 18 IT professionals working in the domain of knowledge management. We decided to use a knowledge café as it motivates and commits participants to take an active role in the process and enables conducting effective brainstorming sessions with a large group of people (Dvir et al. 2004). Further, a knowledge café provides a relaxing environment to discuss matters freely (Kwong et al. 2009). The core principles of a knowledge café meets the purpose of our study: clarifying a concept of interest, i.e. knowledge protection, as well as its importance; exploring meaningful
questions that arise during the exploration of the topic, encouraging personal contribution, as well as gaining deeper insights into the topic (cf. Goldberg et al. 2006). Our goal was to investigate the current state of practice of (1) organizational, (2) technical and (3) performance measures of knowledge protection.

The knowledge café took 120 minutes and comprised three phases (see Figure 3). First, the participants are sensitized for knowledge protection in a 30 minutes session. Here, our risk management framework (see Figure 2) was introduced and distinctions between data, information and knowledge as well as between IT security management and knowledge protection were presented. We further discussed the differences with the group of participants to ensure their understanding. In the second phase, moderated group discussions of 45 minutes took place in three subgroups. Finally, the results were reflected in a joint discussion of 45 minutes with all participants.

For the group discussions we split the group in three subgroups (one for each of the introduced sub goals introduced above) and nominated one volunteer as moderator for each table. The moderator was assigned to one table and thus also for one topic for the entire knowledge café and had to document the results of the group discussion on flip charts. The moderator also present the results for her topic in the final reflection phase. The remaining five people rotated in a 15 minutes interval between the tables. The appointed moderator briefly introduced the topic and the prior results for the participants of the 2nd and 3rd round. In the third phase, the moderators of each subgroup briefly presented the results of the discussion phase for their topic which were then jointly discussed and reflected.
The authors of this paper guided throughout the phases and took notes. Right after the knowledge café, both researchers discussed these notes and documented them in a protocol. This protocol together with the flip charts were then structured and summarized.

RESULTS

The results section is structured according to our three sub goals which we report in the following and reflect them in the light of the related literature.

Organizational measures: There was a consensus within the group of participants that organizational measures are currently the dominant way to enforce knowledge protection requirements. However, the participants were not aware of a systematic knowledge protection initiative, rather all mentioned organisational measures are currently performed in a dispersed way. This is in line with the literature in which it is stated that many organizations nowadays lack a definite strategy for protecting knowledge (Olander et al. 2011).

The most frequent applied measures rated by our participants are contractual measures like non-disclosure agreements, contractual clauses with suppliers, or competitor clauses. Compared to the pertinent literature, we found that contractual measures are also most often
employed in organizations (Hertzfeld et al. 2006), however, are considered as relatively ineffective as their character is rather punitive (Norman 2001), that social control might be more effective than legal recourse (Liebeskind 1997), and that it is difficult and costly to enforce such formal measures (Olander et al. 2011). Also our participants agree that these contractual measures mainly focus on the creation of awareness. Awareness was seen as an important aspect and trainings, similar to those in IT security management, as one important element. Awareness trainings focus, among others, on communication strategies with persons external to the organization, handling of sensitive documents, and usage of social media.

Role concepts and also levels of confidentiality are used to define clear access and communication rights within organizations especially for highly sensitive areas. These measures have also been discussed in the literature (Desouza et al. 2005). Further, release workflows as well as the four-eye-principle are propagated to secure the organizational knowledge. Again, especially the enforcement beyond formal organizational communication channels is considered as a huge challenge. Further, as most of the critical knowledge is in the brains of the employees (cf. Chan et al. 2011), it is mostly transferred verbally and in informal situations (Baughn et al. 1997).

Based on this observation, our interviewees reported that many organizations restrict the usage of social media and cloud services to a selected set of employees, such as marketing or public relationship management. The measure was rated as less effective as people mostly run social software applications on their own mobile devices even during work. Further, the workflows for social media permits are not formally defined. One participant, working in a high-security environment reported that no ICT devices, including mobile phones, cameras, and usb-
sticks are allowed at all. In this regard the access control to organizational facilities in general was also mentioned as one important aspect.

Within the discussion the need for a holistic organizational knowledge protection concept was expressed. The participants recommended that such a concept should be developed and regularly reviewed by a committee. This concept should include a set of compliance guidelines which can be used for knowledge audits.

Technical measures: One major result of the knowledge café was that technical measures currently mainly focus on the protection of documented knowledge. Here it is relatively simple to apply established procedures from IT security management (Desouza 2006). Hence, authorization concepts and their enforcement in content management or document management systems are frequently mentioned. The encryption of communication channels such as telephone or e-mail and of data storage devices such as hard disks, as well as identity management are currently applied.

The enforcement of the prohibition of social media or cloud services by means of technical measures was also frequently mentioned. Whitelists containing allowed applications are used in organisations that perform IT security management more rigidly. Besides, blacklists containing well-known social media and cloud services are also used.

A clearance approach for e-mail communication was also mentioned: based on its classification, a document can or cannot be attached to an e-mail. This is an interesting approach for which we found no evidence in the literature to the best of our knowledge. Further, the group recommended extending this approach also to social media and cloud services as they could easily be used to bypass the restriction of the e-mail attachment.
Performance measurement: Performance measurement happens in three phases in participants’ organizations: (1) design, (2) implementation/test, and (3) sustainability phase. An important insight from the knowledge café was that the participants considered it as crucial, that performance indicators should cover all three phases.

During the design phase, the frame for organizational performance measurement is set. Here, logs of the current landscape are collected and analysed to define an appropriate security concept. In the scope of this, reference frameworks are used for benchmarking purposes. Before implementing the concept, it has to be evaluated. At this level some “pre-audits” are conducted with dedicated KPIs to measure the success of the implementation. Furthermore, the performance measurement concept, as part of security concept, is developed. Thereby, KPIs to measure the success of protecting documented knowledge are defined.

According to the participants, the total cost of ownership is estimated for the security concept during the implementation phase. Here, the ratio of positive tests to the whole number of tests could be a suitable performance indicator for this phase. During this phase, the acceptance of users towards the new security concept should be measured as well. Knowledge protection goals, policies, measures should be evaluated against the perception of opinion leaders within the organization. Another way to measure performance of protection of documented knowledge is the use of an issue-tracking-system. Hence, during implementation, such problem-tracking should be tested by means of a test cases.

During the sustainability phase, the performance of the implemented security concept is measured on KPI level by means of audits. The participants considered user awareness as a central measurement dimension and named the number of incidents as one potential measure.
The monitoring of system logs have been considered as crucial as they give information about technical leaks in systems and hence hint towards points for improvement.

**CONCLUSIONS**

The results of the knowledge café showed that most of the currently applied organizational and technical measures focus on classified documented knowledge. Even though the participants were aware of the necessity of a systematic approach towards knowledge protection, it seems that their organizations lack an overarching knowledge protection strategy. This supports the findings of Olander et al. (2011) who state that this lack becomes apparent through a lack of central coordination of knowledge protection activities. This decentralized coordination leads to the problem that many organizational measures cannot be enforced properly or they can be bypassed easily as there is no clear relationship to an overarching protection strategy. Rather, the major conclusion of the group discussion was that the major benefit of currently applied organizational knowledge protection measures is the creation of awareness.

Only very few technical measures specifically focusing on the specifics of knowledge, most of them focus on well classified information. Further, it seems that risks associated with the rise of social media and cloud services are simply countered with a prohibition of such technology. Only one approach was mentioned in which the restriction takes both a classification of the knowledge container as well as the receiver into account. However, this lack might diminish potential advantages of knowledge sharing within and across organizations. Here, a more sophisticated approach towards the use of social media and cloud services would help organizations to deal with the boundary paradox challenge. Finally, performance measurement is
lacking behind. Due to a missing organizational knowledge protection strategy, a clear and systematic approach to measure performance is difficult or even not considered as necessary.

One major limitation of our study is that the results are not representative as the number of cases is low. Representativeness, however, was not the goal as this study had an explorative character to gain a richer picture of currently used knowledge protection measures. We plan to reach out to a larger sample of individuals and organizations in future studies. Secondly, the results of the discussion phase depended on the volunteered moderator. This, however, was compensated by the final group discussions and the unbiased moderator can also been considered as advantage for this type of explorative research. The integrated risk management framework as proposed by Manhart et al. (2013) would tackle the weaknesses of currently performed knowledge protection measures reported in the knowledge café. In future research we plan to instantiate our risk management framework in an in-depth case study framed by insurance theory (Marshall 1974).

ACKNOWLEDGMENTS

The research leading to the presented results was partially funded by the European Commission under the 7th Framework Programme (FP7) through the PoSecCo project (project no. 257129) and LEARNING LAYERS (contract no. 318209).

REFERENCES


