Chapter 15
A Business-Driven Process Model for Knowledge Security Risk Management:
Tackling Knowledge Risks While Realizing Business Benefits

Ilona Ilvonen
Tampere University of Technology, Finland

Jari Jussila
University of Jyväskylä, Finland

Hannu Kärkkäinen
Tampere University of Technology, Finland

ABSTRACT

This chapter introduces a model to manage knowledge security risks in organizations. Knowledge security risk management is a process that should always be done in connection with the business benefits assessment and realization. The process model presented 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 and is discussed in light of the benefits realization process. The process model 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. It is also a communication tool for managers to identify possible risk sources and sources for business benefits, and as such works as a translation tool in many business contexts.

DOI: 10.4018/978-1-5225-5427-1.ch015

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 studied extensively (e.g. Bolisani & Scarso, 2014; Matayong & Mahmood, 2013; Tzortzaki & Mihiotis, 2014), there is one viewpoint to knowledge that has received less attention until recent years: knowledge security (Randeree, 2006; Shedden, Scheepers, Smith, & Ahmad, 2011). Despite the importance 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; Padyab, Päivärinta, & 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; Padyab, Paivarinta, & Harnesk, 2014) and as a consequence people and their communication are significant sources of knowledge security risks.

Since knowledge security is still in the early stage as a research field, it is reasonable 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 chapter aims to answer the research question "How can organizations manage knowledge risks and reach business benefits of changes in operation at the same time?" The chapter argues that knowledge security risks should be managed in a systematic process in line with managing business benefits and introduce a conceptually developed process for this purpose.

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 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 chapter 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.