Chapter 22
An Integrated Risk Management Framework:
Measuring the Success of Organizational Knowledge Protection

Stefan Thalmann
University of Innsbruck, Austria

Paolo Ceravolo
Università degli Studi di Milano, Italy

Markus Manhart
University of Innsbruck, Austria

Antonia Azzini
Università degli Studi di Milano, Italy

ABSTRACT

Organizational risk management should not only rely on protecting data and information but also on protecting knowledge which is underdeveloped in many cases or measures are applied in an uncoordinated, dispersed way. Therefore, we propose a consistent top-down translation from the organizational risk management goals to implemented controls to overcome these shortcomings. Our approach adopted from the domain of IT security management allows to measure how well knowledge protection is actually pursued in organizations. This affects organizations' abilities to prove compliance to risk management standards, laws, guidelines, or frameworks and creates transparency throughout the whole knowledge protection processes. After introducing our integrated risk management framework, we demonstrate how the technical part of the framework can be implemented by using process mining in a case study of an Italian aerospace company.

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 (Rees et al., 2003). Recently, companies take on great efforts to protect their data and information, spending a lot of money and resources to implement organizational frameworks such as COBIT and also engage with auditors

DOI: 10.4018/978-1-5225-1837-2.ch022

to verify these frameworks. At the same time knowledge management (KM) literature praises sharing of knowledge and investigates how this sharing could be facilitated. However, even if organizations are aware of the negative impacts on the organizational performance when knowledge protection is neglected, it receives little attention in practice and KM literature so far (Jarvenpaa & Majchrzak, 2010; Väyrynen et al., 2013). Hence, it could happen that global organizational risk management goals are implemented rigidly for protecting data and information, and that these goals are all along neglected or implemented in a non-systematic way from the knowledge perspective. Solid strategies for knowledge protection are missing even if they are needed in today´s world in which the importance of knowledge as well as the amount of knowledge threats steadily increase (Alstete, 2003).

Intended knowledge transfer comes along with an increasing number of communication channels, but the control of unintended knowledge transfer is reduced (Hamel et al., 1989). This problem is exacerbated by recent developments in the field of social media and mobile technologies that seem promising to support organizations in their knowledge sharing (Bruck et al. 2012; Santos and Nagla 2012; Wang and Shen 2011), but creates challenges to protect knowledge for specific reasons: Knowledge sharing happens then when devices can be used at home, in the workplace, during transportation periods and during leisure activities (Wang and Shen 2011), blurring the boarders between work and leisure time as well as knowledge sharing for themselves and for the job (Väyrynen et al., 2013) whilst the vulnerabilities of online knowledge sharing are perceived as second order consequences (Jarvenpaa & Majchrzak, 2010). Although these trends imply many opportunities like contribution to an organization's performance and innovativeness (Easterby-Smith et al., 2008), they rise the need of establishing a framework for managing knowledge risks.

Whilst IT security management (ITSM) literature has already recognized the necessity to propose security frameworks, models or guidelines (Rees et al., 2003), KM literature widely neglected this topic so far. Rather, knowledge protection is considered to be a barrier to knowledge sharing (Khamseh & Jolly, 2008) even if empirical research shows that successful knowledge protection significantly enhances organizational performance (Mills & Smith, 2011). However neglecting knowledge protection can hinder innovation or cause replication of ideas by external organizations (Cheung et al., July 2012). Finding a balance between protecting and sharing knowledge is crucial and particularly the concept of sharing also needs to be interpreted from a security point of view (Louw & Von Solms, 2013). Underestimating the importance of balancing protection and sharing of knowledge also impacts the performance measurement in KM. Recently the focus of performance measurement is almost exclusively on knowledge sharing and mostly neglects knowledge protection. As the evaluation of security controls based on KPIs has already been discussed in the ITSM literature (Demetz et al., 2011; Sheldon et al., 2008), similar efforts have been missing for measuring and quantifying the success of knowledge protection.

This paper aims to approach this lack of research by proposing a holistic organizational framework for risk management, incorporating the ITSM as well as the KM perspective. Furthermore, it aims at highlighting its contribution to performance measurement of security controls for KM. First we describe the related work of each of the concepts. Second, we introduce our integrated risk management framework. Then, we demonstrate how this framework can be implemented by using process mining in a case study of an Italian aerospace company. Finally, we conclude our work and give an outlook.