Chapter 12
A Risk Assessment Framework for Inter-Organizational Knowledge Sharing

Ruba Aljafari
University of Nebraska at Omaha, USA

Surendra Sarnikar
Dakota State University, USA

ABSTRACT

Internet-based information, communication, and collaboration technologies are making it easier for organizations and knowledge workers to collaborate across organizational boundaries. However, it is necessary for organizations to monitor, regulate, and build appropriate security mechanisms in collaboration systems to prevent loss of strategic knowledge and competitive advantage. In this chapter, the authors synthesize literature on knowledge sharing and IS/IT risk assessment to present a risk assessment framework that can help organizations identify valuable knowledge assets exposed through collaboration technologies, and assess the risk of knowledge loss, intellectual property leakage, and the subsequent loss of competitive advantage so that appropriate security mechanism can be designed to prevent such a loss.

INTRODUCTION

Organizations are increasingly using collaboration technologies and systems to move towards collaborative inter-organizational network structures. Such network structures are being used to manage various business processes such as supply chain processes, joint product development, customer relationship management, development of industry standards, and for engaging in collaborative commerce. In addition to formalized inter-organizational collaboration mechanisms, organizations and their knowledge workers are also leveraging the powerful capabilities of Web 2.0 technologies such as Wiki's, blogs, discussion forums, social networks and online communities in serving their business needs. Examples of

DOI: 10.4018/978-1-4666-0948-8.ch012

use include interaction with customers in order to generate ideas and feedback as in cases like GM, Domino's Pizza, and Dove or to encourage employees to communicate ideas and experiences (Chui, Miller, & Roberts, 2009).

While knowledge workers continue to leverage such technologies to engage in ad hoc collaboration with customers, vendors, and professional colleagues to exchange knowledge and provide improved services, it is also necessary to ensure that they do not expose strategic organizational knowledge to threats (Fanning, 2007). Web 2.0 technologies are inherently difficult to secure, as they make organizational intelligence more accessible and searchable (Short, 2009). Several news reports and companies have reported cases of intellectual property leakage and loss due to insufficient protection of knowledge assets (Burrows, 2004; Hamm, 2006; Herbst, 2009; Zhen, 2005). Even as companies restrict the use of technologies by using tools such as e-mail monitoring or non-disclosure policies, data and IP leakage is still considered a major risk that is even ahead of viruses and Trojans (Oricchio, 2009; Probasco, 2009; Spring, 2008).

Benefits and risks associated with inter-organizational collaboration and knowledge sharing have been discussed in the literature from a very high level and strategic perspective. Significant work has also been done in the area of information security risk assessment and security mechanisms for inter-organizational collaboration systems. While there are several IT risk assessment models such as the Control Objectives for Information and related Technology COBIT (*COBIT*, 2001) the Information Technology Infrastructure Library ITIL (*Information Technology Infrastructure Library ITIL*, 2001) and the series of information security standards ISO/IEC 27000 (*The Information Security Management Systems Family of Standards*, 2000) their scope is limited to technology infrastructure and data and information assets and does not consider knowledge assets. In their study of identifying risks in e-commerce relationships, Sutton, Hampton, Khazanchi, and Arnold (2008) point that IT governance frameworks do not provide guidelines for assessing inter-organizational risks, as they seem to focus solely on technical issues. Moreover, most information assurance frameworks focus on data assets rather than knowledge. On the other hand, while there are several knowledge management frameworks that help identify and analyze knowledge assets, such frameworks are rarely integrated into existing risk assessment frameworks. There is limited literature that provides a structured process for identifying strategic knowledge assets exposed through collaboration systems, specific risks associated with sharing those assets in inter-organizational collaboration, and strategies for selecting techniques to minimize the knowledge sharing risk in inter-organizational collaboration.

In this chapter, we synthesize on research in knowledge sharing and Information Systems risk assessment and present a framework for identifying strategic knowledge assets and potential threats to the knowledge assets exposed by collaboration technologies. In this framework, we take an integrated approach to address the complexity of business networks or the extended enterprise (Dynes, Kolbe, & Schierholz, 2007). We define knowledge assets as tangible and "intangible assets that encompass the knowledge as well as the ability of an organization to leverage that knowledge. They can also be the technology that facilitates the interaction of the knowledge with the human capital" (Freeze and Kulkarni, 2005). The term risk is used in this study to refer to the potential damage, loss, or negative effect of sharing those knowledge assets. Bayer and Maier (2006) further elaborate on these negative effects by stating that "knowledge risk can be caused by the loss of, unsuccessful intended or unintended transfer of knowledge assets that result in loss or non-exclusivity of these assets".

The framework includes a systematic process through which organizations can identify, value knowledge assets and estimate potential strategic