Knowledge Sharing Security and Organizational Context

Relationship between Knowledge Sharing Security and Organizational Context in the Public and Private Organizations

Emergent Research Forum papers

Azadeh Sarkheyli
Lund University
azadeh.sarkheyli@ics.lu.se

Abstract

One of the most significant current discussions in Knowledge Sharing (KS) is security. Security is an important component in KS, and plays a key role in reducing the risks in KS. However, relatively little study has been performed on KS security in the public and private sectors, and even less in the developing countries. This research intends to find the relationship between organizational context and KS security which have not previously been dealt by other studies, to propose a research model. The potential constructs for the model are identified through literature review. Hence, the research model is divided into three main parts: organizational context, organizational type and KS security. Organizational context includes factors in three dimensions, namely, organizational structure, organizational culture, and information technology. In this study organizational type is identified as a moderating construct. Therefore, this study illustrates the influence of organizational context and type in KS security.

Keywords

Knowledge Sharing Security, Organizational Context, Public Sector, Private Sector.

Introduction

Tiwana (1999) classifies Knowledge Management (KM) in three different processes: Knowledge Acquisition (KA), Knowledge Sharing (KS) and Knowledge Utilization (KU). KA is the process of development and creation of insights, skills, and relationships. KS is the act of disseminating and making available knowledge that is already known, and KU is where learning is integrated into the organization (Tiwana 1999). Alavi and Leidner (2001) stated that KS could be defined as a process. Hence, KS is one of the processes in KM framework apart from knowledge creation, knowledge organization, and knowledge application (Alavi 1997; Argote 2012). On the other hand, it can also be viewed as one of the elements in KU cycle when combined with KA and KU (Tiwana 2000).

KM security includes risk management in KM strategy and ultimately increases the value of knowledge. KM security impacts the organization by managing risks such as reluctance to share significant knowledge, disclosure of knowledge to intended parties, and losing, or misapplying critical knowledge (Zyngier et al. 2004). Knowledge risk is defined as operational risk caused by a loss, unintended diffusion, insufficient transfer and limited quality of knowledge assets and results in a lack or non-exclusivity of these assets (Fitzgerald 2009). To distinguish the components of the model, various variables are determined through a literature review. Three main parts are specified as KS security, organizational context, and organizational type. The research is conducted for implementation of the proposed model in the public and private organizations. Hence, the main research question is "what is the relationship between KS security and organizational context in the public and private organizations?"
Knowledge Sharing Security

Risks of KM are divided into three main categories: risks of KA, risks of KS and risks of KU (Liu et al. 2010). Therefore, by assessing the related risks, knowledge loss, knowledge disclosure, insufficient knowledge transfer and limited knowledge quality are identified as the risks of KS. Knowledge loss is related to risk of losing knowledge, such as trade secrets, core technologies and other types of strategically important knowledge (Ritala et al. 2015; Baughn et al. 1997; Hannah 2005). Thus, it is expected that KS security negatively affect probability of knowledge loss by rules concerning e.g., email and document retention planning, documentation and reduction of dependencies as well as measures that reduce the probability of fluctuation, e.g., comparable wages, leadership, incentives (Desouza and Vanapalli 2005; May and Plummer 2011; Williams and Hardison 2013). Knowledge disclosure is assumed that probability and exposure of knowledge diffusion is reduced by deploying KS security such as access control, patenting knowledge, non-disclosure agreements or alliance agreements (Zander and Kogut 1995; Norman 2004; Desouza and Vanapalli 2005; Cheng 2011; Nelson 2015). Limited knowledge quality is identified as one of the risks of KS. Hence, implementation of KS security through accessibility of IT infrastructures, applicability or correctness of documented knowledge could positively affects knowledge quality (Eppler 2003; Cheng 2011; Shiroyama et al. 2012).

Organizational Context and Knowledge Sharing Security

Aspects of organizational context that have been held to be relevant to KS security were examined. Three primary concepts of organizational context are considered as organizational structure, organizational culture and IT (Robey and Azevedo 1994; Lemon and Sahota 2004; Islam et al. 2015; Kim and Lee 2006).

Organizational Structure

Two factors of organizational structure are common in KM research which are organizational support and reward systems (Eisenberger et al. 1997). In addition to organizational support, reward systems that provide members incentives to shape their behavior or improve their performance in learning are also essential (Davenport and Prusak 1998; Connelly et al. 2012). Improving employee learning and creating environments where the exchanges of ideas are shared helps to increase the likelihood of KS and prevent the risks of KS (eg. formal support, informal sanction and promotion). Hence, mangers from different units need to understand the importance of KS security and how it can be used to support the business and not obstruct it.

Organizational Culture

Social Interaction and Trust of organizational culture receiving consistent attention related to KS security. Social interaction is a channel for information and resource flows which represents the strength of the relationships, the amount of time spent, and the frequency of communication among members. (Tsai and Ghoshal 1998).

Trust refers to a set of specific beliefs primarily pertaining to the integrity, benevolence, and ability of another party (Chiu et al. 2006). Blau (1964) states that trust is essential for the social exchange process. Trust creates and maintains exchange relationships, which in turn may lead to the sharing of good quality knowledge. When trust exists between two parties, they are more willing to participate in cooperative interaction. High relationship capital will enhance KS and security between employees through trust (Randeree 2006).

Information Technology

IT for connecting the information and knowledge of the organizations are significant. Hence, IT increases KS through computer networks, and electronic bulletin boards for instance (Alavi and Leidner 2001). IT Security Policies are categorized in policies of IT. The area of end-user security behaviors in organizations has gained an increased attention and these safety policies are provided to different types of users in the organizations to establish requirements for each individual to follow in order to safeguard the organization and administrative information and knowledge resources (Knapp et al., 2009).
Research model and Hypotheses

This research proposes a conceptual model of organizational context that includes factors in three dimensions, namely, organizational structure (organizational support and reward systems), organizational culture (social interaction and trust), and IT (IT application usage and end-user focus). This research indicates that organizational type is a construct that it cannot ignore in investigating KS security. Organizational type addresses the concept of public and private organizations in developing countries. Public organization is a governmental organization with the permanent contracts for the employees. On the other hand, a private organization is typically a non-governmental organization containing members with temporary contracts. Therefore, this construct of the proposed model as a moderator could influence on the connection between organizational context and KS security which is necessary to design and develop KS strategy. Therefore, the research hypotheses which are related to these constructs are listed as follows (see Figure 1).

Hypothesis 1 (H1a–H1f): Organizational context is positively associated with KS security.
Hypothesis 2 (H2a–H2f): Organizational type moderates the relationship between the organizational context and the KS security.

Research Approach

The research focused on three main phases: 1) understanding the relationship between organizational context and KS security in the public and private organizations, 2) identifying the components of the research model and 3) empirical studies based on the first and second phases. Therefore, a sequential mixed method consisting of a qualitative phase to explore the model and KS security, and a quantitative phase to validate the model will be adopted for this research. Literature review of findings from the previous studies on KS security is collected in order to explain variability in findings across the studies. Hence, several studies found issues affecting the KS security based on the organizational context which are summarized in this study. The next step to validate the model includes several case studies (public and private) will be provided that illustrate the relevance of organizational context with KS security. Questionnaires will be used to collect data from case studies. Thus, in this study, developing an instrument for survey and testing the research model will be useful for future research.
Conclusion

This study illustrates the impact of organizational context and type on KS security. Organizational support, reward systems, social interaction, trust and relationships, IT security policies, and end-user security are considered as organizational context as our base to develop a model that includes organizational type as a moderator. The results of this research will be valuable for managers in organizations that influence the success of implementing KS security. We think that research in this area especially in the public organizations could have different results. However, to provide qualitative and quantitative support for this research, using case study research strategy could be suitable in order to examine KS security based on the organizational context and type.

REFERENCES


