Knowledge Management and Information Technology Security Services

Pauline Ratnasingam
University of Central Missouri, USA

INTRODUCTION

With the explosion of the Internet and Web technologies as a medium of exchange, issues such as knowledge coordination problems, knowledge transfer problems, and knowledge reuse problems related in IT security knowledge management have been growing exponentially. These problems arise from the complexities faced by individuals, groups, and organizations in recognizing the nature of knowledge needed to solve problems or make decisions.

Knowledge management (KM) provides a formal mechanism for identifying and distributing knowledge. It is the discipline that focuses on capturing, organizing, sharing, and retaining key corporate knowledge as an asset (McManus & Snyder, 2002). KM ensures that the right knowledge is available in the right representation to the right processors (humans or machines) at the right time for the right costs (Holsapple & Singh, 2005). Benefits of proper KM include improved organizational effectiveness, delivery of customer value and satisfaction, and added product and service innovation. There is no reason to believe that IT security will be an exception in the context of KM and IT. It has been recognized that the first step in the KM process is to identify or define knowledge needs**.** This article aims to discuss the role of knowledge management categories, namely *knowledge resources, knowledge characteristics, knowledge dimensions, and stakeholders in IT security* and their relationship to *security services*. We develop a theoretical framework by integrating IT security services pertaining to confidentiality, integrity, authentication, non-repudiation, access controls, and availability of IT systems with the knowledge management categories. The study extends the theory on knowledge management and the importance of maintaining IT security.

We conclude the article with the contributions of the framework to theory and practitioners leading to directions for future research. The next section introduces the categories of knowledge management and IT security services. We begin with the definition of knowledge management from previous research. We then provide a discussion of the categories of knowledge management leading to the development of an integrated IT security framework of knowledge management.

BACKGROUND

Knowledge management (KM) is the generation representing storage, transfer, transformation, and application, embedding, and protecting organizational knowledge (Alavi & Leidner, 2001). In fact, KM is an IT practice that is implemented in the faith that doing so will lead to higher levels of organizational performance (Ribiere & Tuggle, 2005).

Nonaka and Tekuichi (1995) introduced the four modes in the knowledge management process, namely *socialization, externalization, combination, and internalization.* While socialization converts tacit to tacit knowledge, externalization converts tacit to explicit knowledge, and internalization converts explicit to tacit knowledge. Socialization is where sharing of IT security experiences among employees and other stakeholders occur that in turn creates tacit knowledge. Externalization is the articulation of tacit knowledge into explicit concepts (documenting knowledge). Combination aims at systemizing the concepts into a knowledge system. New knowledge can be created by combining different forms of explicit knowledge and reconfiguring existing information through sorting, adding, combining, and categorizing. Finally, internalization embodies knowledge into tacit knowledge and is closely related to learning by doing, when socialized, externalized, and combined knowledge is internalized into employee's tacit knowledge bases, and it then becomes a valuable asset.

Knowledge management is the application of knowledge in an organized systematic process of generating

Table 1. Definitions of knowledge management and its relationship to KM categories and IT security services

Source	Definition of KM and its relationship to KM Categories	**Relationship to IT Security** Services
Barth (2001)	It is a realization that who and what you know are assets of the organization (stakeholders of IT security knowledge and knowledge dimensions)	Identifies how authentication mechanisms are applied
Hult (2003)	The organized and systematic process of generating and disseminating information, and selecting, distilling, and deploying explicit and tacit knowledge to create unique value that can be used to achieve a competitive advantage (knowledge characteristics)	Identifies how integrity and confidentiality mechanisms are applied
Koch (2002)	Applying knowledge manipulation skills in performing knowledge manipulation activities that operate on the organization's knowledge resources to achieve organizational learning and projections. (knowledge resources)	Identifies how access controls and non-repudiation mechanisms are applied

and disseminating information, and selecting, distilling, and deploying explicit and tacit knowledge to create unique value that can be used to achieve a competitive advantage. Alavi and Leidner (2001) suggest that there are many unresolved issues, challenges, and opportunities in the domain of knowledge management. Previous research suggests that the dimensions of knowledge management include knowledge resources, knowledge dimensions, knowledge characteristics, and stakeholders of knowledge.

Table 1 provides the definition of knowledge management and its relationship to knowledge management categories.

MAIN FOCUS OF THE ARTICLE

The main focus of this study is to explore the impact of knowledge management in IT security. We categorize knowledge management as *stakeholders of IT security knowledge, knowledge dimensions, knowledge characteristics, and knowledge resources* discussed next. This is followed by a discussion of factors that make up the IT security services, namely *confidentiality, integrity, authentication, non-repudiation, access controls, and availability.*

Stakeholders of IT Security Knowledge

Maintaining IT security effectiveness is no longer the sole responsibility of the IT security officer but also the business unit managers' and the chief executives' responsibility. The stakeholders of IT knowledge are the "right people" who should possess IT security knowledge to maintain confidentiality, integrity, and availability. Everyone legitimately interfacing with an organization's information system should know the role they play in supporting the security services, and the knowledge needed to execute the role. Organizations should develop a systematic procedure for identifying and classifying legitimate users with similar knowledge needs. Stakeholders can be classified into whether they are internal or external to an organization. External stakeholders will include the customers, suppliers, trading partners, and government bodies; audit and tax firms may have very different knowledge needs than internal employees. Internal employees can be classified into those who directly work with the IT system and those who do not. The chief information officer (CIO), chief information security officer (CISO), network and systems administrators, internal auditor, database administrators, and programmers are those that directly operate with the firm's IT systems.

Knowledge Dimensions

Knowledge dimensions refer to the *right information* that needs to be imparted to the stakeholders in order to maintain the confidentiality, integrity, authentication, non-repudiation, and availability of IT systems. These are categories of knowledge needed by the stakeholder to make effective decisions regarding IT security. Some of the broad common dimensions of knowledge taken from multiple sources needed for IT security are illustrated in Table 2. (See Maguire, 2002, and Solomon and Chapple, 2005). The dimensions include information security planning, information security policy development, information security project manage-