Security-Based Knowledge Management

Shuyuan Mary Ho
Syracuse University, USA

Chingning Wang
Syracuse University, USA

INTRODUCTION

As knowledge is recognized as intellectual (or intangible) assets that can enhance an organization's competitive capability, how to effectively manage knowledge assets has become an important issue in the information age (Alavi, 2000). Literature in knowledge management (KM) emphasizes issues on knowledge creation, knowledge codification, knowledge sharing, and knowledge utilization; however, security perspectives on assuring knowledge confidentiality and knowledge integrity are left unaddressed.

This article takes an initial step to address different perspectives of security centric knowledge management. This article first presents the background of security-based knowledge management. It then discusses sources of security threats in knowledge-based organizations and identifies challenges in four aspects of knowledge management practices, which are culture-based, strategy-based, content-based (or standard-based), and technology-based, along with a discussion of 10 corresponding security domains. Real-world cases are intertwined with the challenges faced by knowledge-based organizations. This article ends with further envisioning the future trends of the security-based knowledge management.

BACKGROUND

While knowledge management enables collaboration within an organization to retain and share knowledge and experience, threats to knowledge confidentiality and integrity have raised corporate concern.

Threats against organizations are multi-faceted. Hackers and crackers have greatly threatened information[1] transmission over the virtual world such as the Internet, intranet and extranet. Many corporations have applied multi-layered security solutions to prevent threats of this kind. System-layered security solutions include system logs, host-based intrusion detection, file encryption, identity-based, or role-based access control. Network and infrastructure-layered security solutions include firewall, virtual private network, public key infrastructure, cryptography, network-based intrusion detection, and intrusion prevention. Physical separation of the networks is seen as the fundamental practice to protecting information assets. One of the best examples would be the practice of the de-militarized zone[2] (called DMZ). In the social context, personnel with a knowledge base of the corporate assets could pose potential threats to the organizations. Corporate regulations, best practice, and ethical codes could be security solutions to threats of this nature.

With the advance of information technology, threats to information security have come to corporations with increasing frequency and subtlety, and so information security should be an emphasis in the field of knowledge management for the new information era.

SOURCES OF INFORMATION THREATS

Threats against information security can be intentional or unintentional. These threats can be further differentiated into internal threats and externals threats. Sources of security threats are tabulated in Table 1.

External Threats

In a networked environment, intentional threats from outsiders include attacks from hacker/crackers (Harris, 2003).

Table 1. Sources of threats to information security

	Intentional	Unintentional
External	Malicious Hacker/Cracker; outsider ID theft	Natural disasters
Internal	Personnel fraudulence; unauthorized modification/leakage of knowledge/information[1];	System failure

These attacks include man-in-the-middle, Trojan Horse, denial-of-service (DOS), logic bombs, viruses, and so forth. These attacks could cause malfunctions of the systems and result in loss in terms of time and money. For instance, *The New York Times* suffered attacks in 1998, which resulted in its web servers being compromised and its Web front page replaced.

Identification (ID) theft is another type of external threat. The purpose of those malicious hackers in this scenario is to steal personal information such as social security numbers, credit card numbers, or to conduct banking transactions without authorized permission. Additionally, they could commit identification (ID) fraud by falsely presenting stolen identification in exchange of goods and services in this virtual e-commerce world. These misconducts could cause huge losses and creditability damage to innocent victims.

On the other hand, external threats from natural forces such as earthquakes, tornadoes, or tsunamis are generally unintentional and thus become difficult to prevent in advance. Damages caused by natural forces could be devastating and hard to restore. The tsunami that devastated Southern Asia in December 2004 was an example of this kind.

Internal Threats

Threats from insiders are subtle and complex (Hayden, 1999; Park & Ho, 2004). Like a double-edged sword, the knowledge from internal personnel could bring beneficial advantages, but also ironically, could bring potential security threats as well to an organization (Benkoil, 1998; Powell & Rosenberg, 1987). For example, in 1985, Jonathan Pollard, a U.S. Navy intelligence analyst, was arrested for passing classified U.S. intelligence information to Israel. The Israeli government was then able to analyze U.S. intelligence infrastructure such as the locations of facilities and identities of intelligence agents. As such the General Accounting Office (GAO) reported in 1993 that insiders' abusive use of the National Crime Information Center (NCIC) for personal reasons had threatened the safety of U.S. citizens (Benkoil, 1998; Powell & Rosenberg, 1987). Insider threats have been statistically increased since late 1980, and, more so, the cost of loss from the insider threats has exceeded the threats from outsiders (Hayden, 1999; Park & Ho, 2004). Normally insiders are not interested in sabotaging hardware systems or applications but in obtaining critical information and accessing the internal level of resources. Due to the insider threats, the paradigm has shifted toward a more sophisticated and security centric collaborative environment

On the other hand, infrastructure failures such as power outage and destruction of infrastructural devices such as routers and switches are seen as unintentional internal threats. These threats bring up issues on operational site redundancy, system maintenance, and information preservation.

ASPECTS OF KNOWLEDGE MANAGEMENT AND INFORMATION SECURITY

Knowledge management can be classified into four aspects: culture-based, strategy-based, content-based, and technology-based (Alavi & Leidner, 1999; Oostveen & van den Besselaar, 2004). These four aspects represent four major themes in managing knowledge. Each theme of knowledge management has related security concerns. International Information System Security Certification Consortium, Inc. (known as (ISC)2) has identified 10 domains of information security that would assure knowledge management practices in organizations. These 10 information security domains include law, investigation and ethics, risk assessment, operations security, business continuity planning, physical security, security architecture technology standards, access controls, telecommunications and network security, applications security, and cryptography. These aspects are not mutually exclusive but overlap one another. We map the 10 domains of information security (Hansche, Berti, & Hare, 2004; Harris, 2003) with four aspects of knowledge management identified in literature (Table 2).

Table 2. Conceptual map of knowledge management aspects and domains of information security

Aspects of Knowledge Management	Corresponding Domains of Information Security
Culture-based	Law, Investigation and Ethics
Strategy-based	Risk Assessment Physical Security Operations Security Business Continuity Planning
Standard-based	Security Architecture
Technology-based	Access Controls Telecommunications & Network Infrastructure Security Applications Security Cryptography