Chapter 136
Secure Knowledge Management

S. Upadhyaya
University at Buffalo, USA

H. Raghav Rao
University at Buffalo, USA

G. Padmanabhan
GE Transportation Systems, USA

Category: Organizational and Social Aspects of Knowledge Management

INTRODUCTION

As the world is getting more and more technology savvy, the collection and distribution of information and knowledge need special attention. Progress has been made on the languages and tools needed for effective knowledge management and on the legal issues concerning the consumption and dissemination of critical knowledge. From a business perspective, a knowledge-management system (KMS) within a firm generally strives to maximize the human-capital utilization and profitability of the firm. However, security is becoming a major issue revolving around KMS; for instance, the KMS must incorporate adequate security features to prevent any unauthorized access or unauthorized dissemination of information. Acquiring the information that one needs to remain competitive while safeguarding the information one already has is a complicated task. Firms must balance the advantages of openness against its inevitable risks, and maximize the efficiency of electronic communication without making it a magnet for intruders. One must integrate offense and defense into a comprehensive strategy, and scholars have suggested that it is time to integrate intelligence and security imperatives with other knowledge-management strategies and processes (Barth, 2001).

Since the widely reported attacks on knowledge repositories in 2001 (e.g., Amazon was hit by denial-of-service attacks and the NIMDA virus hit financial markets), many organizations, especially the U.S. government, have increased their concern

DOI: 10.4018/978-1-59904-931-1.ch136

about KMSs. With the advent of intranets and Web access, it is even more crucial to protect critical corporate knowledge as numerous individuals now have access to the assets of a corporation. Therefore, we need effective mechanisms for securing data, information, and knowledge as well as the applications (Thuraisingham, 2003, 2004).

Security methods for knowledge-management systems may include authentication or passwords, cryptography programs, intrusion-detection systems, or access-control systems. Issues include insider threat (protecting from malicious insiders), infrastructure protection (securing against subversion attacks), and establishing correct policies, refinement, and enforcement. KMS content is much more sensitive than raw data stored in databases, and issues of privacy also become important (Thuraisingham, Chadwick, Olivier, Samarati, & Sharpston, 2002).

Asllani and Luthans (2003) surveyed over 300 knowledge managers about their job roles and found little or no evidence of security issues being considered in their jobs; their primary role was focused on communication within the organization. This article about secure knowledge management raises a number of issues in this critical area of research that need to be tackled by knowledge-management practitioners. The following sections focus on three important aspects of secure knowledge management: secure languages, digital-rights management (DRM), and secure content management (SCM).

BACKGROUND

A firm exists as a repository of knowledge over time (Zander & Kogut, 1995). Knowledge management is the methodology for systematically gathering, organizing, and disseminating information (Morey, Maybury, & Thuraisingham, 2003) in a firm. It essentially consists of processes and tools to effectively capture and share data, as well as use the knowledge of individuals within a firm. Knowledge management is about sharing information more freely such that firms derive benefit from such openness.

Secure knowledge-management (SKM) systems can be described in terms of the three *C*s: communication, collaboration, and content. SKM systems act as a gateway to the repository of intellectual content that resides within an organization. SKM systems need to source and/or provide access to knowledge that resides in multiple machines across an organization or multiple organizations for collaborative efforts. Secure languages are utilized to transfer information safely. At the same time, digital-rights management becomes critical in cross-organizational transfers of knowledge, while access control and identity management play an important role in securing the knowledge-management system. A framework for secure knowledge management is shown in Figure 1 as two interlinked, triangular chains: The larger chain focuses on security, knowledge, and management, while the smaller triangular chain (with dotted links) focuses on content, communication, and collaboration. Different aspects within the smaller chain include secure content management, digital-rights management, and secure languages. This article focuses on the interarticulation of the different concepts in the triangles.

SECURE LANGUAGES

In order to communicate securely and collaborate with one another, organizations need to use secure languages. These languages can be implemented to enhance the security of knowledge-management systems. Some of these are detailed in the following sections.

Security-Assertion Markup Language

The security-assertion markup language (SAML) can secure the KMS from insider or outsider