SECURITY AND PRIVACY ISSUES IN A KNOWLEDGE MANAGEMENT SYSTEM

Chandramohan Muniraman, Meledath Damodaran, Amanda Ryan

University of Houston-Victoria

Abstract

As in any information management system security issues are critical in Knowledge Management Systems (KMS.) Many security threats and risks that apply to information systems in general apply to KMS too. In addition, there are a few unique security risks posed by KMS’s very nature of sharing and providing different means of accesses. In this study we will discuss the security issues in a KMS - in particular the issues in the KMS of a large software development organization providing services to organizations in various industries. We will look at some security requirements and discuss security solutions to handle these situations.

Keywords: Knowledge Management System, security, privacy, security solutions

Introduction

Software development companies develop Knowledge Management Systems (KMS) to help their software development project teams and departments share and reuse knowledge about projects, project plans, procedures, intuitive solutions, technical issues and functional processes. This information often pertains to project management activities and development activities including requirements, design, tools used, and standards and procedures. Knowledge Management Systems are developed to ensure that institutional information about each project are available for use by all.

Information about various functional subject areas should also be available for use by members of different virtual teams. There could also be an infrastructure or medium for forums wherein subject matter experts could share their expertise and opinions. Different components of KMS range from a simple system with stored in files to a complex system with a heterogeneous array of subsystems with sophisticated search options. Typically, KMS’s employ a KM portal as a central point of access for its component systems.

In general information in an organization may exist in:

- Applications
- Technical support help desk systems
- Business procedures
- Process documents
- Technical design documents
• Software tools and systems user manuals
• Individuals’ knowledge of all these
• Forums

But they may need to be context sensitized to be relevant and appropriate for a situation. In addition, a means may provided for people to easily update it or add related additional information and their personal knowledge. Then search capabilities may be provided for easy and quick access to requested information. Finally this may be placed in a portal with all other tools, information and other often used links, so that everything is available in one place for the user. A fully functional KMS would be much more sophisticated with many additional features and options.

Security Issues and Requirements

The very nature of KMS raises many security issues, related to operations such as in adding, updating, sharing, and providing information and knowledge. In addition, since a KMS may not be thought of as a critical system by the upper management or even the technical personnel, generally due importance may not be given to its security. So a few KM “security champions” may be needed, whose job it is to educate others about the importance and even cost-effectiveness of a “secure” KM system.

Sources of Information

Information exists in many different sources and places, such as in files, technical design documents, process flow documents, procedures and policies. Much information exists in individuals’ personal knowledge, experience and intuition. Different procedures and technologies must be followed to extract and deploy information from these various sources. Files and documents may need to be centrally located and shared. Additionally data may have to be stored in databases. People accessing these might be in different geographic locations.

Providing Accesses

Providing access of the individual components to users of the KMS raises several issues, such as who all should be given access to edit or update and add or post information in different parts of the system. These would then in turn become issues in managing its security.

Access control is not only important to prevent unauthorized access and consumption of information but also to provide relevant role-based information to individual users. Too little information or too much or irrelevant information could severely affect system usage.
Client Data

Information about sensitive and critical customer data that are parts of prior projects may need to be sanitized before making it a part of a KMS. Otherwise, it may result in a breach of confidentiality of customer information.

Stakeholders

The stakeholders may include sponsors, end users, developers, analysts, designers, project managers, quality control, and deployment teams. KMS is expected to help them with useful and appropriate information to perform various tasks and to support their decision making and problem solving tasks. All of them would expect the system to be available as needed, and provide current information, technical guidance, resolution details of prior issues, schedule details, project details, requirement specifications, functional process flow, and so on.

Impact

Sometimes the information stored in a KMS represents trade secrets or specially developed procedures and techniques which must be protected from unauthorized employees and external users. Otherwise it could threaten the company’s competitive advantage in the market. Also, hackers and intruders could steal, delete or change its accuracy. All these could cause loss of revenue or reputation.

Sometimes a part of an internal procedures could be quoted out of context if some employees or outsiders could accidentally gain access to just a part of it - without knowing the full context. This could cause legal issues and negative publicity, and so eventually may have to disclose full details, which could compromise their specialized knowledge or competitive business advantage.

If the system is unavailable or does not provide accurate and timely information, the company’s work or the quality of its products and services may be affected.

On the other hand, if the system it is not easily accessible to users or if there is too many restrictions in terms of security, users might not use it at all, defeating the very purpose of a Knowledge Management System.

Security Requirements

Different components of KMS should be identified, and their information sources, extraction methods, usage patterns and access levels must be studied in order to understand the underlying security issues associated with these components. The following are typical components of a KMS:

- Body of Knowledge
- Process Assets
Quality System Documentation
Discussion Forum
The People Knowledge Map (Yellow Pages)
Best Practices Seminars
Departmental Knowledge Portals
Online Learning Material
Online Documentation

The software tools used to implement these systems include: databases, file servers, email server, site server and various development tools. The individual users typically use desktops with web browser, office automation software, and email client software.

Security requirements should be considered before the design, development and implementation of the KMS, and of the KMS portal. It should include an analysis of the following two components:

- Data and functional or business side issues, and rules.

The criticality and sensitivity of the functions implemented and of the data must be considered, and their security requirements must be specified.

- Technological components.

The technological components and systems chosen to build the KMS should be analyzed for their inherent potential security issues, and security requirements that address these issues must be specified.

Security Needs of Specific KM Components

Body of Knowledge, Departmental Knowledge Portals, Process Assets and Quality System Documentation might involve proprietary information based on company’s many years of research and development, and so must be protected from unauthorized access and copying to external systems.

Discussion Forum might have context sensitive information and involve maintaining the privacy of the contributors, and so this must be protected from external systems, intruders and other teams.

People Knowledge Map (Yellow Pages) might have personal contact details of the company’s management and professional staff, and perhaps other sensitive data as well, that needs to be secured to protect their privacy.

Best Practices Seminars, Online Learning Materials, and Online Documentation may involve more general information, industry standards, and best practices. This may not be critical information from security point of view, but their availability and currency should be ensured.
Database and Servers

Data stored in databases must be analyzed to provide database security features for protecting them, depending on their sensitivity. They must also consider providing security features for the file servers, email server and site server.

Integration

When integrating all these components and technologies in a KMS, some security gaps could open up and these must be addressed. These include granting access to databases from other systems, providing server administrative access to component systems, and allowing update information in one system from other systems.

Portal Access: From Intranet or the Internet

An important decision must be made regarding the access to the portal: whether to give access to the portal from intranet only, which needs connecting to the company’s network first; or whether to give access from the internet, which could allow users to access it conveniently from anywhere, but would imply the need for additional protection. Also, since the portal could be used to access many other systems, the inter-access mechanism must be carefully designed with security built-in from the beginning.

Security Solutions for KMS

Based on the security issues and requirements we discussed we will now discuss some solutions for these. The solutions will be in terms of policies, procedures, change management, source code management, operations or business process controls, security features, configurations, options, and protection systems. Of utmost importance is the realization among the builders of the KM system and the KM champions that security must be designed in, from the very beginning, and not “added on;” that security is not only an after-the-fact “IT issue” but an issue that must start with careful identification of security requirements and carried through during design, implementation, testing and deployment.

Non-technological Procedures and Policies

Acceptable usage guidelines and security policies must be developed for the KMS as a whole and for each of its component systems. Users must be required to read, understand and accept these terms.

Procedures must be developed for each function. Source code controls, and change management procedures and processes must be developed and followed. Appropriate approval levels must be set. For adding, updating and posting information procedures and processes must be set, with the required approval for each system component and its various operations.
Procedures must be developed for allowing individuals to add or update relevant information. Before it is posted it must be verified by authorized people or subject matter experts. Different delivery mechanism must be utilized for different kinds of information. Also, decisions must be made regarding whether each department is responsible for maintaining information in their area or others should be allowed to add or update that.

Policies and procedures must be developed for usage, maintenance and system administration. When modifying or moving new programs and configurations they should first be tested by developers in a development environment, and then by user groups in a user acceptance environment before deploying them to production environment.

IT administrators responsible for the KM infrastructure should keep themselves up-to-date and current on all available relevant technology and study all aspects of prospective products when it comes time to add to, upgrade or replace components in the system’s infrastructure, so that the best decision may be made when making a selection for hardware and software purchases.

**Encryption Tool for Files and Other Information Stored in the KMS**

File encryption systems and options are the standard way to secure files. Operating system features or third party tools or utilities may be utilized for file encryption. For data stored in database, database security features should be used. These include granting individual accesses to roles, rules for selecting and changing passwords based on policy, and enabling audit trails and logging. Very sensitive information could be encrypted using database encryption features.

Hardware encryption appliances that encrypt data on servers and back-up tapes are available from various vendors, including Decru (DataFort), Kasten Chase Applied Research, NeoScale Systems and Vormetric. They sit on the network, encrypting and decrypting data as it passes through from hosts and enterprise-wide storage resources. They can also convert raw files into encrypted data silos. They use ASICs to increase performance.

**Security Tools for Confidentiality of Proprietary Information**

First, a determination has to be made as to who will have access to the different components of the KM system and the levels of access. This is followed by a determination of the right type of user authentication and user verification. User authentication ensures that only authorized users access the system; whereas user verification ensures that the user is who they say they are. For authentication, encryption systems could be used. For information integrity and confidentiality, message by message authentication and encryption systems may be used. This applies to system components and functions such as body of knowledge, process assets, quality system documentation, departmental knowledge portals, the people knowledge map (yellow pages), and parts of...
discussion forum. This kind of information could be deployed in a separate part of the system; it will be easier to implement security controls this way. Also, sensitive client information; and any related reports, evaluations and estimates should be kept confidential and protected.

Security tools exist for assuring confidentiality of shared info, such as company proprietary, departmental proprietary etc. One could employ, for example, brokered authentication on the transport layer for data confidentiality using X.509 certificates and HTTPS, implement transport layer security using SSL, and configure the Web service virtual directory to use SSL and require client certificates.

Secure Portal

If the portal is a kind of single sign-on system, meaning that from here users could access other component systems with the same credentials without the need to log on to it separately, then additional protections should be provided.

Also, if the users could access it from the internet - then highly secure connections must be implemented. If it could only be accessed from the intranet then the VPN or network security protections could provide this protection.

Authentication systems with encryption should be implemented to provide secure access to the portal. SSL systems could be used for providing connection to the portal system.

Various levels of security are often provided by vendors of portal software. The IBM WebSphere Portal (Galic, 2004), a very popular example, provides three layers that make up the portal system:

- A presentation layer for user configuration, web user interface, and transcoding
- A portal services layer for user management, administration & security, application integration, document management, etc.
- An information access layer for integrating with other enterprise resources
- Includes native security functions for authentication, authorization, and auditing and can integrate with other security management products

Reliability, Currency, Usefulness and Quality of Information

Reliability should be high because after some initial use, users would routinely expect to use the system for any and all needs. Data must be current in most components, otherwise the very purpose the system would be defeated. Personalization could be effective in providing relevant and useful information for the individual teams, and its users. Also the users must be able to access only the individual systems to which they have been authorized.
Quality of information will be ensured by maintaining change controls. Also persons should be authorized, and approvals must be required to add and update information. This should be followed strictly, especially for systems whose information is relied upon by users for critical work. But for forums, and sharing of new ideas, all users could be encouraged to post relevant information.

Workflow and categorization functionality may be added to the KM system applications to ensure that necessary safeguards are part of a change management system. Workflow provides a structured manner in which changes take place to the data; otherwise, most recent changes always take precedence over accuracy. Categorization provides the following: It determines specific categories according to guidelines for establishing what changes will have the greatest impact on the KM system and possibly even the organization so that these changes will be of priority for review or evaluation.

**Content Management**

Information should be timely, relevant to each system component, and sufficiently accurate as per the needs and usage of the component system. Information sources should be constantly monitored and KMS should be updated as per the policy. This information upload could also be automated and scheduled for many of the components.

**Change Management**

Controls should be developed and enforced for changing the information – in each part of the system, based on its functional needs, criticality and usage. Change management controls must be implemented for changing the programs and source code or configurations, and testing them in separate environments.

**Access Controls and Policies**

Security policies and usage guidelines for the KMS must be developed as part of the overall company security policy. Procedures and rules for each function and component should be developed. Approvals levels and rules must be there for adding and updating information. Access controls should be put in place for each function and system depending on users’ team, role, position, work or projects. Information must be made accessible based on their roles and needs. Limited access control by users/participants may be determined according to role-based parameters. Then they could personalize the relevant information from this allowed list, based on their changing needs as they move between different projects or phases of development.

Also, accesses to add or update this information may need to be given to individual users or their roles based on their organizational position, expertise or criticality of the information. In forums everybody could be given access to add or update information, but in knowledge bases only certain persons with expertise in that area could be given
access. These decisions could affect the accuracy, integrity and relevancy of the information – in the long term.

The organization should continuously monitor use of the KM system to determine patterns of use and overall performance levels, in order to make adjustments to the policies to accommodate for special issues or requirements.

Copies of security and privacy policies concerning the KM system and its use should be posted on the KM portal and in other appropriate locations in order to heighten policy awareness. KM system users should be periodically surveyed to determine if there are any adjustments that need to be made to the KM system and/or its governing policies.

Commercial software packages such as the Tivoli Access Manager (Karjoth, 2003) provides policy-based control services for applications, especially those on the web. It can be centrally managed and may be integrated with the IBM WebSphere Portal (Galic, 2004) to supplement the security functions already present on the portal. It also provides the following:

- End-to-end security
- Policy-based security
- Application level data protection
- Distributed web-based administration

**Network Security**

Much can be said about network security, but only some general but important remarks will be made here. Network security protections depend on the allowed access method for the portal, whether internet or intranet. If it is only allowed from the intranet then general protections for securing a network could be ensured. In case VPN access is provided it could handle this. But if access to portal is allowed from the internet through web browser, then additional security features must be provided. The network security systems such as firewall and intrusion detection systems could be used. These must be configured to protect against hacking, denial of service or gaining control of other systems through KMS or portal. The network must be tested periodically to identify any weaknesses and/or vulnerabilities so that they may be fixed.

**Ease of Implementation and Reliability**

For each of the above, the tools selected should be easy to implement and maintain. At the same time, they should be reliable for the critical functions such as portal authentication. Also the implementation should seamlessly integrate the different systems automatically, with the user not aware of these at all. Except for critical functions such as authentication and confidentiality, the system should also be easy to access and use.
Cost-Benefit Analysis

Implementation of authentication, encryption and other systems may be expensive, but cost should not be a major factor for secure access to the KM portal, especially from the internet, due to the importance of maintaining confidentiality of sensitive information, and of ensuring the integrity of critical information. But in other parts of the system, depending on the functional design and security risks identified, cost-effectiveness of the different alternative methods or technologies should be studied.

Doing an effective cost-benefit analysis for security systems is not easy because many benefits are intangible. Studies have shown that the data that is stored in company data stores degrade at a rate of 2 percent per month when data change is not managed. Other studies show that as a result of inaccurate and low-quality data, U.S. businesses lose about $600 billion a year. Although taking the proper precautions to protect their KM system may be somewhat costly for an organization, these costs would likely pale in comparison to their potential losses.

Summary

In summary, we conclude that there are major security issues in a Knowledge Management System. A KMS may not be thought of by many as business critical, but it could be a very important part of the overall operation and management of the organization. Besides, a KMS is a valuable asset, which might have involved the investment of much effort, time and cost to rebuild the system. Moreover, compromise of a KMS component may result in loss of productivity and revenue, decreased morale of users, and loss of reputation in terms of reduced support or development performance.

Authentication and encryption systems should be utilized for providing secure access to the KMS or portal. Some of the information might not be very critical and could be protected through general operating system or database features. But other more critical and sensitive information and components must be protected by specific, more effective security solutions. Also, privacy issues must be considered from the beginning. A security policy, procedures, usage guidelines and rules for each functional component must be developed.

References