7-9-2010

A Risk Assessment Framework for Inter-Organizational Knowledge Sharing

Ruba Aljafari
University of Nebraska at Omaha, raljafari@unomaha.edu

Surendra Sarnikar
Dakota State University, sarnikar@acm.org

茅|Sprouts Working Papers on Information Systems ISSN 1535-6078

A Risk Assessment Framework for Inter-Organizational Knowledge Sharing

Ruba Aljafari
University of Nebraska at Omaha, USA

Surendra Sarnikar
Dakota State University, USA

Abstract
Internet-based Information, Communication and Collaboration technologies are making it easier for organizations and knowledge workers to collaborate across organizational boundaries. However, it is necessary for organizations to monitor, regulate and build appropriate security mechanisms in collaboration systems to prevent loss of strategic knowledge and competitive advantage. In this paper, we present a risk assessment framework that can help organizations identify valuable knowledge assets exposed through collaboration technologies, and assess the risk of knowledge loss, intellectual property leakage, and the subsequent loss of competitive advantage so that appropriate security mechanism can be designed to prevent such a loss. We present an illustrative scenario to demonstrate the feasibility of the framework, and describe a prototype decision support system for automating the risk assessment process.

Keywords: Knowledge sharing, Collaboration, Risk assessment

Permanent URL: http://sprouts.aisnet.org/10-29

Reference: Aljafari, R., Sarnikar, S. (2010). "A Risk Assessment Framework for Inter-Organizational Knowledge Sharing," . *Sprouts: Working Papers on Information Systems*, 10(29). http://sprouts.aisnet.org/10-29

1. INTRODUCTION

Organizations are increasingly using collaboration technologies and systems to move towards collaborative inter-organizational network structures. Such network structures are being used to manage various business processes such as supply chain processes, joint product development, customer relationship management, development of industry standards, and for engaging in collaborative commerce. In addition to formalized inter-organizational collaboration mechanisms, organizations and their knowledge workers are also leveraging the powerful capabilities of Web 2.0 technologies such as Wiki's, blogs, discussion forums, social networks and online communities in serving their business needs. Examples of use include interaction with customers in order to generate ideas and feedback as in cases like GM, Domino's Pizza, and Dove [10] or to encourage employees to communicate ideas and experiences as in cases like Microsoft and Apple [32].

While knowledge workers continue to leverage such technologies to engage in ad hoc collaboration with customers, vendors, and professional colleagues to exchange knowledge and provide improved services, it is also necessary to ensure that they do not expose strategic organizational knowledge to threats [16]. Web 2.0 technologies are inherently difficult to secure, as they make organizational intelligence more accessible and searchable [40]. Several news reports and companies have reported cases of intellectual property leakage and loss due to insufficient protection of knowledge assets [6, 21, 24, 47]. Even as companies restrict the use of technologies by using tools such as e-mail monitoring or non-disclosure policies, data and IP leakage is still considered a major risk that is even ahead of viruses and Trojans [32, 35, 41].

Benefits and risks associated with inter-organizational collaboration and knowledge sharing have been discussed in the literature from a very high level and strategic perspective. Significant work has also been done in the area of information security risk assessment and security mechanisms for inter-organizational collaboration systems. While there are several IT risk assessment models such as the Control Objectives for Information and related Technology COBIT [26], the Information Technology Infrastructure Library ITIL [9] and the series of information security standards ISO/IEC 27000 [42], their scope is limited to technology infrastructure and data and information assets and does not consider knowledge assets. In their study of identifying risks in e-commerce relationships, Sutton, Hampton, Khazanchi and Arnold [45] point that IT governance frameworks do not provide guidelines for assessing inter-organizational risks, as they seem to focus solely on technical issues. Moreover, most information assurance frameworks focus on data assets rather than knowledge. On the other hand, while there are several knowledge management frameworks that help identify and analyze knowledge assets, such frameworks are rarely integrated into existing risk assessment frameworks. There is limited literature that provides a structured process for identifying strategic knowledge assets exposed through collaboration systems, specific risks associated with sharing those assets in inter-organizational collaboration, and strategies for selecting techniques to minimize the knowledge sharing risk in inter-organizational collaboration.

In this paper, we build on past research in knowledge sharing and Information Systems risk assessment to propose a framework for identifying strategic knowledge assets and potential threats to the knowledge assets exposed by collaboration technologies. In this framework, we take an integrated approach to address the complexity of business networks or the extended enterprise [15]. We extend the Freeze and Kulkarni [19] characterization of knowledge assets to define knowledge assets as tangible and “intangible assets that encompass the knowledge as well as the ability of an organization to leverage that knowledge. They can also be the technology that facilitates the interaction of the knowledge with the human capital”. The term risk is used in this study to refer to the potential damage, loss, or negative effect of sharing those knowledge assets. Bayer and Maier [2] further elaborate on these negative effects by stating that “knowledge risk can be caused by the loss of, unsuccessful intended or unintended transfer of knowledge assets that result in loss or non-exclusivity of these assets”.

The proposed framework includes a systematic process through which organizations can identify, value knowledge assets and estimate potential strategic risks by sharing those assets. The framework consists of five essential components that focus on (1) identifying knowledge sharing practices, (2) identifying knowledge assets, (3) identifying collaboration technologies that expose these knowledge assets, (4) identifying the risk associated with the knowledge assets, and (5) a Dempster-Shaefer based model for quantifying the risks.

The rest of the paper is organized as follows. Section 2 provides background and context on inter-organizational collaboration. Section 3 reviews relevant literature in inter-organizational collaboration and knowledge sharing and information technology risk assessment. Based on the findings from the literature review, we generate the requirements of the proposed framework in Section 4, and provide a detailed description of the proposed framework in terms of the required steps and the objective, method and output of each step. Section 5 presents the design of a decision support system based on the framework followed by an illustrative case that demonstrates the use and feasibility of this framework in Section 6. Finally, Section 7 concludes the paper with a summary of contributions and opportunities for future research.

2. BACKGROUND

Previous research has suggested that firms are better off when they use and re-use mature internal as well as external ideas in different domains, because this is more cost effective than creating the same ideas from scratch [23]. Organizations are therefore increasingly exploring inter-organizational knowledge sharing arrangements within an environment that allows them to build valuable intellectual capital and knowledge assets [22].

In Figure 1, we present a typical knowledge sharing scenario in inter-organization networks in the context of the value chain of a computer manufacturing organization, where inbound, manufacturing, and outbound logistics bring together suppliers, manufacturers, customers, retailers and other partners. The labeled arrows between different entities show the flow of different types of knowledge that may take place between the entities.

As can be noted from the figure, knowledge sharing can appear at any stage or sub-process within the value chain of a company. For example, component design knowledge can be transferred between a Semi-conductor chips manufacturer and the computer manufacturer. Best practices and benchmarking knowledge can be transferred between different computer manufacturers. Customer support agents may share product design knowledge with customers and receive customer requirements knowledge. While several knowledge sharing activities may have beneficial impacts on the company, harmful knowledge sharing activities are also possible. Inadvertent disclosure of sensitive business knowledge or information could be an example of such activities [27]. Computer engineers and knowledge workers at the computer manufacturer, for instance, may share product design knowledge inadvertently with competitors through communities of practice or ad hoc collaborations. Such harmful transfer of knowledge may also occur through regular customer support interactions, or interactions with suppliers and vendors resulting in a strategic risk to the computer manufacturer.

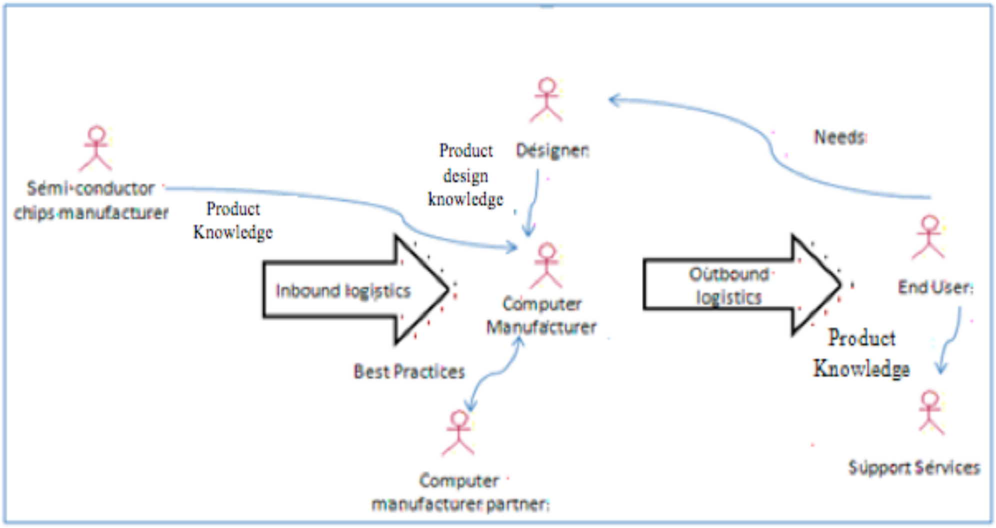


Figure 1 Knowledge sharing in the computer industry

Collaboration among organizations can take the form of strategic alliances, where knowledge sharing and acquisition are critical for creating customer value and improving competitive advantage [29]. However, knowledge sharing may be problematic in such systems since it involves diverse relationships and participants in this system may have conflicting interests. For example, risks pertaining to knowledge sharing may arise when knowledge is transferred to other projects that may benefit competitors of the firm that owns the original product or when the partner decides to move to innovating the basic product [1].Thus, a more systematic approach is required to help organizations in identifying and assessing risks and therefore be able to design the most effective security measures. Such a framework will enable organizations to take a more proactive approach in a given knowledge sharing scenario.

3. LITERATURE REVIEW

We classify relevant literature into two main categories that include inter-organizational collaboration and information technology risk assessment.

3.1 Inter-organizational Collaboration and Knowledge Sharing

Inter-organizational knowledge sharing has been analyzed from three different perspectives, technical, behavioral and strategic. The technical perspective is mostly focused on designing and implementing secure systems and architectures for collaborative knowledge sharing. The behavioral perspective includes research that explores behavioral issues related to collaborative knowledge sharing, such as trust and social ties among participants in the same collaboration system. Finally, the strategic perspective analyzes inter-organizational knowledge sharing benefits and risks from a high level. We further explore the strategic perspective as it provides key insights necessary for the identification and assessment of knowledge sharing risks. The importance of the strategic perspective is risk management illustrated by Schaak, Dynes, Kolbe, and Schierholz [38] who develop an IS risk oriented outsourcing model based on the notion that the vocal point of risk management should be the business mission rather than focusing directly on IT security issues. The model integrates best practices in IS risk management and abstractions of the outsourcing process in order to identify and manage IS risks with outsourcing partners. In order to analyze the strategic impact of knowledge sharing, Levy, Leobbecke, and Powell [28] proposed a game theoretic approach to analyze inter-organizational knowledge sharing among small and medium enterprises (SME). In an empirical investigation of their model, they find that SME's are good at knowledge creation but are poor at knowledge retention and need to recognize the value of knowledge shared to retain competitive advantage. Most firms depend on legal contracts and policies to control knowledge sharing. However, developing such policies to ensure high level of control and flexibility at the same time is a difficult problem [5]. Moreover, organizations may acquire and use knowledge that is beyond the boundaries of the legal agreement governing specific knowledge assets. For example, partners in a strategic alliances can learn from each other business and management skills that they were lacking individually [30].

According to Das and Teng [11] there can be two types of risks in strategic alliances, that include relational risk and the performance risk. Performance risk is basically related to the probability that alliance objectives may not be met despite good relations between partners [11]. Such risks may arise because of new entrants to the industry, demand fluctuations, changing government policies, and lack of competence of partner firms. In the context of supply chain management, Dynes, Brechbühl, and Johnson [14] analyze information security in the extended enterprise by focusing on two types of risks. Those include, risks pertaining to internal IT systems and information as a result of integrating the supply chain and risks to a firm's ability to produce products as a result of supply chain disruptions caused by information infrastructure events. The relational risk arises because of the fact that partners may have their own individual interests that may conflict with those of other partners. This may result in opportunistic behavior, as described by [11,12], such as cheating, distorting information or knowledge and appropriating shared resources. In the supply chain, for instance, access to valuable logistics information can be used to seize control of cargo [46]. Even in cases where legal agreements exist, partner organizations may acquire and use knowledge not covered by legal agreements for competing purposes. Other knowledge sharing risks may include diffusion of the firm's knowledge [4], as the value of the shared knowledge diminishes, which results in a potential loss of competitive advantage [34]. In strategic alliances, predicting and managing conflicts, which may be important sources of risk, is usually overlooked [33]. While there are many benefits to knowledge sharing, organizations need to weigh the benefits against risks pertaining to knowledge sharing. A summary of the risks related to knowledge sharing is illustrated in Table 1.

Table 1 Risk factors

Risk factor
Unauthorized learning
Unauthorized sharing of sensitive knowledge
Unauthorized use of knowledge asset
Manipulation of knowledge asset
Appropriation of knowledge asset

3.2 Information Technology Risk assessment

In addition to literature on strategic risk in alliances and collaborations, another related area of literature includes the Information Technology risk assessment techniques. The main focus of Information Technology risk assessment literature is the securing of IT assets from external and internal threats. There are several IT risk assessment models proposed in literature [8, 9, 26, 36, 42, 43, 44] A typical IT risk assessment process begins with identifying data, information and technology assets that might be exposed to risk and quantifying threats associated with them [36]. This process can be challenging since evaluation in this domain can be highly subjective [17], as managers assign personal judgments on related risks. After identifying those vulnerable assets and determining risk, experts can design, select, apply the best protection mechanisms and evaluate them in an iterative manner [17, 18]. Examples of IT Risk Assessment models include the Policy Framework for Interpreting Risk in E-business Security (PFIRES) [36], the Risk Management Guide for Information Technology Systems by [43], OCTAVE [8], and COBIT [26].

Although there are risk assessment frameworks for information technology assets, and literature on collaboration risk and strategic issues in inter-organizational knowledge sharing, currently there is no structured process that can help organizations analyze risks in inter-organizational knowledge sharing and Web 2.0 collaboration and sharing environments. Organization's knowledge assets, which may be tacit or explicit, are vulnerable to threats when exposed to external organizations through collaborative settings. Thus, organizations need to analyze different aspects related to knowledge sharing in these settings. For instance, is there a risk that partners can gain access to knowledge that the sharing firm uses in other business areas? What kind of knowledge is being diffused through employee blogs or employee participation in technical discussion forums? Is the knowledge diffused strategic to the company? What are the most appropriate protection mechanisms in such situations? Currently there exists no framework that can help managers address these aspects. In the next section, we build on past literature in Information Technology risk assessment to develop a framework that can help in assessing risks of knowledge sharing.

4. RISK ASSESSMENT FRAMEWORK

A firm must go through a systematic methodology to assess inter-organizational knowledge sharing risk. In this paper, we extend previous risk assessment methodologies such as the NIST Risk Management Guide for Information Technology Systems [43] and the PFIRES by [36] to develop a risk assessment framework that is suited for the inter-organizational knowledge sharing case. Since knowledge is often shared using information and communication technologies, we begin by building upon Information Technology risk assessment frameworks and extend them to incorporate knowledge assets and risks associated with knowledge sharing. In the next section, we present the requirements of the framework followed by a detailed description of the risk assessment process.

4.1 Requirements

The main objective of the framework is to provide a structured process for managers to identify and evaluate risks pertaining to knowledge sharing. We have identified three key factors from strategic knowledge sharing and risk management literature that influence the utility and success of the proposed framework. The factors include identifying and recognizing the content that is shared, the context in which knowledge is shared, and the inherent subjectivity in valuing knowledge assets and assessing risks.

A key element of the risk assessment process is the systematic identification of the assets that need to be protected [18, 26, 36, 46]. As organizations increasingly engage in inter-organizational collaborative projects, it is important that they recognize the knowledge assets that are involved in the collaborative processes, their characteristics, and the strategic advantage provided by the knowledge asset to the organization [5, 7]. Identification of knowledge assets as well as their strategic value is essential to retain strategic advantage as organizations balance benefits and risks of knowledge sharing in co-operation and competition situations [28].

In addition to identification of knowledge assets, the context in which the knowledge assets are shared has important implications for assessing knowledge sharing risks [5]. The knowledge sharing context includes the business processes in which knowledge is being shared, the entities involved, and the associated collaboration and communication technologies. Communication and Collaboration technologies are important conduits for knowledge transfer and different technology features can act as filters or enablers of knowledge transfer.

Mentzas and Apostolou [31] for instance, emphasized the need for understanding the role of electronic media in analyzing inter-organizational knowledge transfer. Bayer and Maier [2] consider the role of collaborative use of information systems in knowledge transfer. In their study of information sharing in supply chain management systems, [46] identify information technology solutions as important elements in ensuring the security of information sharing. Thus, identifying collaboration technologies through which potential knowledge transfer takes place is an important requirement of the risk assessment process.

The subjectivity in experts' judgments in estimating risks also needs to be reduced by deploying sufficient analytical capabilities. Since risk assessment involves judgment and decision making at some point in the process, a common problem associated with such situations is the subjective nature of those judgments. Subjective judgments could negatively affect the quality and the reliability of the risk assessment process as a whole [20, 44]. Thus, there is a need for controlling this problem in order to generate "bias-free" risk estimates.

4.2 Risk Assessment Process

In this section, we describe tasks in the risk assessment process in terms of the objective, method, and output. An overview of the proposed risk assessment framework is presented in Figure 2.

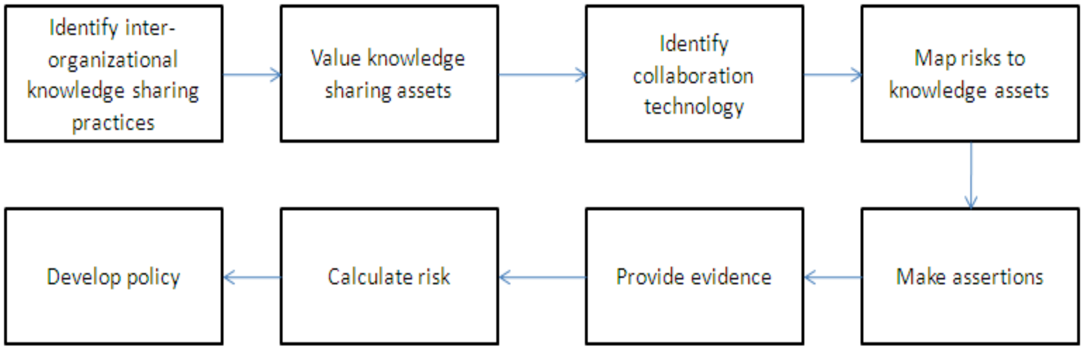

Identify inter-organizational knowledge sharing practices
Value knowledge sharing assets
Identify collaboration technology
Map risks to knowledge assets
Make assertions
Provide evidence
Calculate risk
Develop policy

Figure 2 Risk assessment process

4.2.1 Identify inter-organizational processes

Objective:

The objective of this step is to identify organizational processes that may involve sharing of knowledge assets with external entities. This step is based on the notion that boundaries of the IT system must be defined in the early stages of the assessment process [43]. An organization can identify the extent of knowledge sharing activities by identifying the business process that provide the context through which knowledge assets are shared. This step follows a top down approach that assists managers by starting with the main process and then narrows down the focus towards assets involved and their associated risks.

Method:

- Identify key business processes executed by organizational units using the value chain model, for instance, or any business model that clearly represents the firm's business processes and its relationships with suppliers, customers, and competitors.
- Identify organization's members and external partners involved in those business processes.

Output:

The final output of this step would be a list of business processes and associated internal as well as external entities.

4.2.2 Value knowledge assets

Objective:

The main objective of this step is to identify the most valuable knowledge assets that need to be protected. Organizational knowledge assets may reside in people, documents, or technology artifacts. In this step, managers begin by identifying and classifying knowledge assets. This is important because being specific about knowledge assets can help in identifying related threats and later in identifying securing policies.

Method:

- One approach that can be used to identify knowledge assets is to sketch a tree diagram with different types and repositories of knowledge resources, so that managers can clearly spot and identify knowledge assets [3]. Knowledge can be stored in individual's or expert's mind as tacit knowledge or in groups as collective and synergistic [3]. It can also be encapsulated in artifacts such as practices (e.g. procedures and rules), technologies and knowledge repositories. Figure 3 illustrates this approach.
- Identify strategic knowledge assets by assessing the (a) value, (b) rareness and (c) imitability of each knowledge asset. This approach is based on the resource-based view of knowledge and designed to measure the competitive advantage provided by the knowledge asset [7]. The value of a knowledge asset is a measure of the extent to which the asset enables the firm to sense and respond to opportunities and threats in the business environment. The rareness of the knowledge asset measures the extent to which competing firms may possess similar knowledge and imitability refers to the difficulty of

obtaining or imitating the knowledge resource by other organizations that do not own it. In this framework, a manager could value knowledge assets using these criteria on a scale from 1 to 5, with 5 indicating the highest value and 1 indicating the least value.

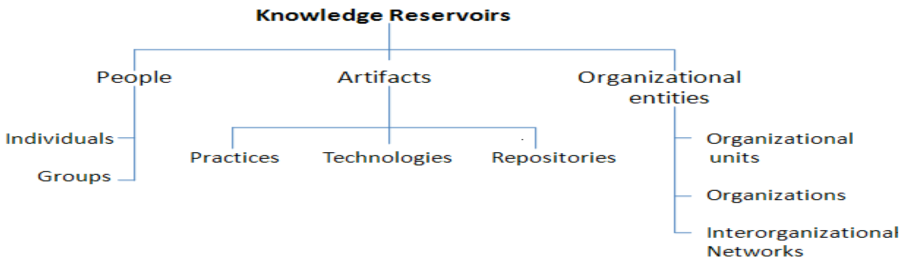


Figure 3 Reservoirs of knowledge (Adapted from Becerra-Fernandez et al. [3])

Output:

The output of this step would be a ranked list of knowledge assets based on the previously discussed criteria. These assets will be used later on in the risk assessment process as the unit of focus.

4.2.3 Identify collaboration technologies

Objective:

The objective of this task is to identify the medium or collaboration technology through which knowledge could be transferred to an external entity. Examples of such technologies include, but are not limited to, e-mail, Wiki's, blogs, and discussion boards.

Method:

The method used to accomplish this task involves identification of collaboration technologies used to share a knowledge asset in the context of the previously identified processes, internal as well as external entities and strategic assets.

- The technology is identified in the context of a process. For example, the requirements collection template might be shared with customers via a consultant/customer portal, whereas, it is shared with vendors and affiliated developers via a project management website/code versioning system during the development process.

Output:

The output of this step is a Process-Technology-Asset matrix that can help document the knowledge asset vulnerabilities. Questions evaluating risks will be generated later on based on elements in this matrix.

4.2.4 Map risks to knowledge assets

Objective:

The objective of this step is to identify potential threats to strategic knowledge assets in a given context. In this step, the manager identifies which of the risks factors previously identified in Section 3.2 apply to the knowledge assets used in a particular business process.

Method:

- List potential threats to the given knowledge assets. Threats arising due to knowledge sharing include unauthorized learning, unauthorized sharing, unauthorized use, manipulation, and appropriation of knowledge asset.

Output:

The output of this step is a list of applicable threats to a given combination of processes, strategic knowledge assets, and collaboration technologies.

4.2.5 Make assertions

Objective:

The main objective of this process is to make assertions on the risks pertaining to sharing knowledge assets in the context that was generated by the previous steps. In order to accomplish this objective, the following method is proposed.

Method:

- For each knowledge asset, make assertions, as per the evidential reasoning model of Dempster-Shafer theory [13, 39], on the vulnerability of knowledge asset to the identified threats through the given technology. For example, best practices are not vulnerable to unauthorized sharing through employee blogs. The following step then estimates the extent to which this assertion holds true given the evidence.

Output:

The final output of this step is a list of assertions for each knowledge asset that relates the knowledge asset to different technologies and potential threats.

4.2.6 Provide evidence

Objective:

The main objective of this step is to estimate the extent to which the assertions developed in the previous step hold true by evaluating the current measures, if any, in place to protect the knowledge assets from the identified threats. To accomplish this objective, the following method is proposed.

Method:

- The manager identifies the different mechanisms in place to protect the knowledge assets from the different threats identified in the previous step and enters subjective judgments as to the extent to which the mechanisms reduce the risk of specific threats to the knowledge asset. For example, consider the threat of unauthorized sharing for a best practices knowledge asset through an extranet portal. In order to evaluate the assertion that “sharing best practices through extranet is not vulnerable to unauthorized sharing by the external entity”, the manager may identify the mechanisms in place to protect the knowledge asset from unauthorized sharing as non disclosure agreements, access control mechanisms and digital rights management techniques.

- Then, the manager or an expert can input his/her own judgment about the effectiveness of the given techniques in protecting the knowledge asset from unauthorized sharing. Such judgments are captured on a 0-1 scale and are expressed as a degree of belief in support of the assertions, in support of the negation of the assertion and a degree of uncertainty. Delphi methods can be used to help achieve consensus among experts or analysts, and therefore, avoid the effect of subjective judgment when the values are assigned [44].

Output:

The output of this step is an evidential reasoning model that includes assertions and risk likelihood estimates from multiple experts combined in one model. This model will group these estimates in a hierarchical way in order to calculate the overall level of risk in the next step.

4.2.7 Calculate risk

Objective:

The main objective of this step is to calculate the overall level of risk by integrating estimates provided by experts in the previous step. This objective can be accomplished by following an analytical method that is based on the Dempster-Shafer theory to calculate risks [13, 39].

Method:

- The Dempster-Shafer theory is based on the notion of combining separate pieces of evidence to calculate the probability of an event. It is a generalization of the Bayesian theory of subjective beliefs and is widely applied in diverse domains including information systems risk assessment [44]. The overall level of risk is calculated based on weights assigned for evidences within each assertion. The numbers associated with evidence and assertions such as the belief supporting the assertion and the belief negating the assertion can be assigned, as mentioned previously, by experienced managers and analysts.

Output:

The output of this step would be the overall level of risk for each knowledge asset based on experts’ estimates provided in the earlier step. Following the risk calculations, a ranking of knowledge assets based on the level of risk associated with sharing each knowledge assets through a particular technology is presented. For example, the risk of sharing a particular knowledge asset via technology X may be higher than sharing the same knowledge asset via technology Y.

4.2.8 Develop policy

After the overall level of risk is calculated, the manager/s needs to develop a security policy in order to mitigate these risks. Mitigation efforts include technology solutions such as those described in [3], or policy and legal solutions. One way to mitigate risk, for example, is to focus on evaluating the reputation of potential partners, as explained in [2], to help in anticipating opportunistic behavior.

5. A DECISION SUPPORT SYSTEMS FOR ASSESSING KNOWLEDGE SHARING RISKS

In this section, we present the design of a decision support system for knowledge sharing risks based on proposed the risk assessment framework. The decision support system implements the proposed risk assessment framework and includes analytical capabilities for ranking strategic knowledge assets, automatically developing a evidential reasoning model, and calculating risks based on the Dempster-Shaefer theory [13, 39].

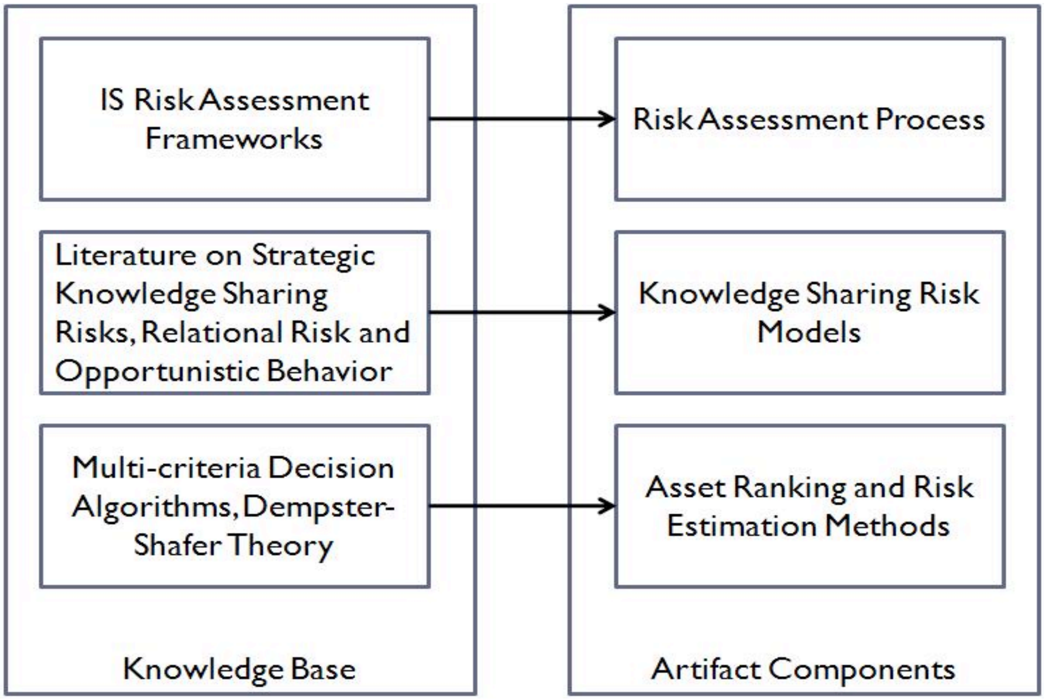

IS Risk Assessment Frameworks
Risk Assessment Process
Literature on Strategic Knowledge Sharing Risks, Relational Risk and Opportunistic Behavior
Knowledge Sharing Risk Models
Multi-criteria Decision Algorithms, Dempster-Shafer Theory
Asset Ranking and Risk Estimation Methods
Knowledge Base
Artifact Components

Figure 4 System components

The basic components of the system, as shown in Figure 4, include an implementation of the risk assessment process, a knowledgebase of knowledge sharing risks for mapping knowledge assets to potential threats, multi-criteria decision algorithms to rank strategic knowledge assets and Dempster-Shaefer theory based algorithms for risk estimation. The design includes an interactive user interface to enable the manager to input information on knowledge assets and displays the evidential reasoning model as well as summary risk reports and recommendation. Figure 5 illustrates an activity diagram that highlights the risk assessment tasks.

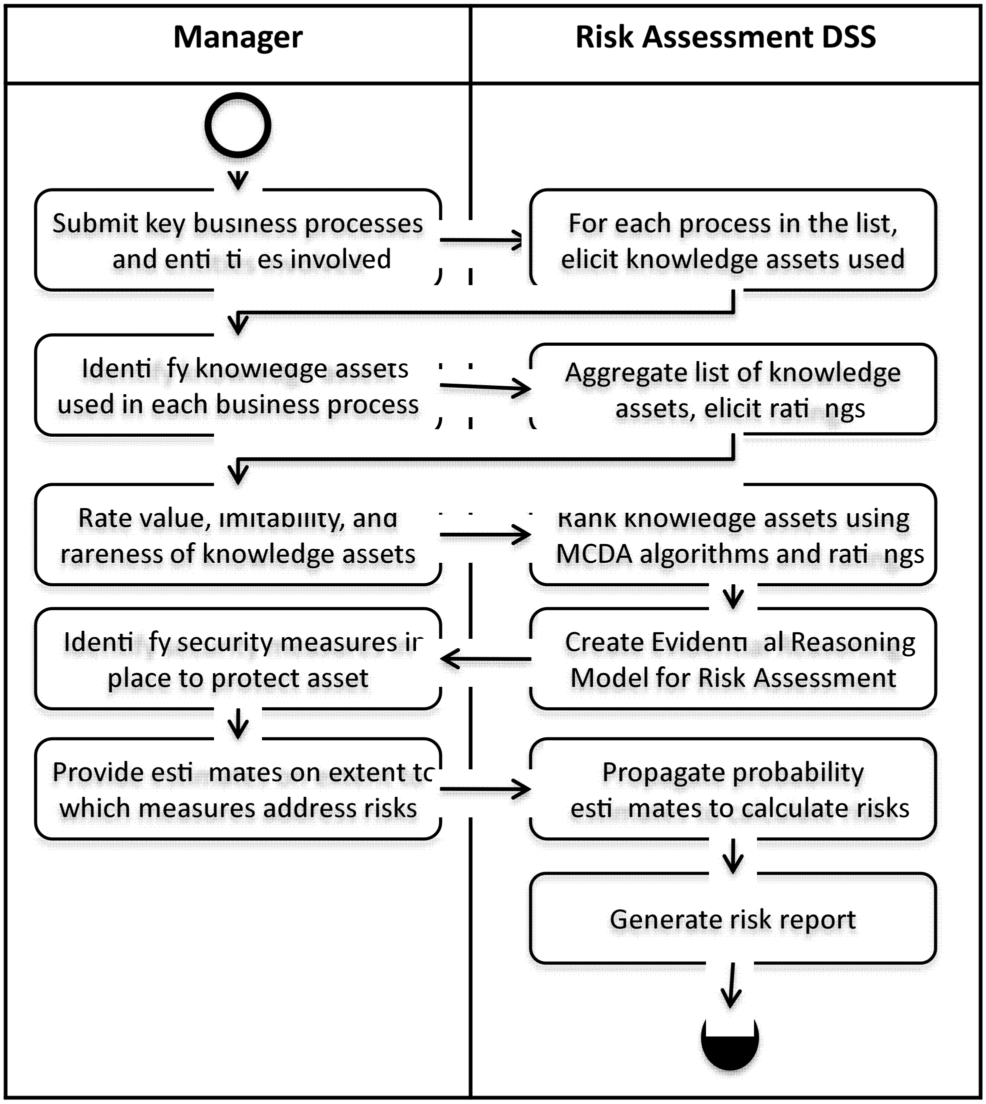

Manager
Risk Assessment DSS
Submit key business processes and entities involved
For each process in the list, elicit knowledge assets used
Identify knowledge assets used in each business process
Aggregate list of knowledge assets, elicit ratings
Rate value, imitability, and rareness of knowledge assets
Rank knowledge assets using MCDA algorithms and ratings
Identify security measures in place to protect asset
Create Evidential Reasoning Model for Risk Assessment
Provide estimates on extent to which measures address risks
Propagate probability estimates to calculate risks
Generate risk report

Figure 5 Activity flowchart

As can be noted from the logic illustrated in the previous figure, the process starts by creating a profile for a particular business unit. The profile includes basic information such as the business unit name, number of companies and employees involved, and key processes. The next step would be to identify internal as well as external entities involved and the knowledge assets used in each of the processes followed by identification of technologies used to share those assets. The list of knowledge assets is then presented to the manager to elicit ratings on the value, imitability and rareness of the knowledge assets. The ratings are then processed by an AHP-based multi criteria decision algorithm [37] that ranks the knowledge assets based on their strategic value. Using a pair-wise comparison matrix, the knowledge assets are compared to each other with respect to the value, imitability and rareness criteria and the overall score for a knowledge asset is determined by combining its priority scores for each criteria. The knowledge asset with the highest score is ranked as the most valuable asset.

Next, the system automatically develops an evidential reasoning model with assertions based on a knowledgebase of knowledge sharing risks, information on strategic knowledge assets, and the technologies through which they are shared. The process for generating the evidential reasoning model is shown in Figure 6. Specifically, it begins with a main assertion developed for each knowledge asset to represent the extent to which sharing the knowledge asset is secure. As in [2], the formal representation of the main assertion can be given as

A_i (Sharing) = {(Secure, X), (Not Secure, Y)}

Where A_i (Sharing) denotes the assertion made on a particular Asset i, Secure and Not Secure denote the evaluation grades, X is the value or extent to which sharing A_i is secure, and Y is the value or the extent to which sharing A_i is not secure. The main assertion is then further decomposed into more detailed assertions that capture the risk of sharing the particular knowledge asset via a particular technology. Next, another level of sub-assertions is developed to decompose the knowledge sharing risks into the specific threats identified in Table 1. The manager then identifies mitigating measures currently in place to address the knowledge sharing risks and estimates the extent to which the mitigating measures address the knowledge sharing risks. Examples of mitigating measures include signing non-disclosure and non-compete agreements and using access control mechanisms. For each knowledge asset, a belief function is generated to assess risk factors by propagating across the model probability estimates on the extent to which the mitigating measures address the underlying risk factors. Finally, the system analyzes the information and outputs different reports that rank the assets based on their strategic value and overall risk to the knowledge asset, risk components and technology sources of the risk.

1. **Identify the set of strategic knowledge assets**
2. **For each strategic knowledge asset A_i, create a main assertion regarding its overall security A_i (Sharing) = {(Secure, X), (Not Secure, Y)} where X and Y are unknown variables that represent the extent to which the knowledge asset is assumed to be secure or not secure.**
3. **For each main assertion about Ai, create a sub-assertion that identifies the technology through which the asset is shared and could be a sources of potential risks.**
4. **For each sub-assertion A_i (Sharing through Technology T), create a new sub-assertion that maps the parent sub-assertion to knowledge sharing risks identified Table 1.**
5. **For each sub-assertion of the form A_i (Sharing through Technology T is vulnerable to risk R), identify mitigating measures and elicit probabilities on the extent to which the mitigating measures prevent a particular threat, do not prevent a particular threat, and the level of uncertainty of the effect of the mitigating measure.**
6. **Propagate the probability estimates for each sub-assertion to the parent sub-assertions using Dempster-Shaefer rule and calculate the values for X and Y in Step 2.**

Figure 6 Process for building evidential reasoning model

6. ILLUSTRATIVE EXAMPLE AND EVALUATION

In this section, we present an illustrative example to demonstrate the feasibility and utility of our proposed framework and then discuss the extent to which our proposed framework satisfies the requirements discussed previously in Section 4.2.

6.1 Illustrative example

ABC Software is a mid-sized software development consultancy that develops customized software applications, extensions, and modules to third party software platforms based on client requests and market needs. The company, whose customers predominantly include small and mid-size businesses, specializes in serving the needs of specific industries such as rental companies, and food services industry, as well as specialty development platforms such as mobile computing apps and social networking apps. A sample list of products developed by the company for different vendor platforms is given in Table 2.

Table 2 Sample products of ABC software

Lotus Notes	Joomla CMS
Sync App for Android	Event Management Module
Sync App for iPhone	Auction Module
Lotus Notes CRM Database	ActiveDirectory Extension
ACL Security Manager	Log Analysis Module

As a part of its business process, the company's engineers and employees participate in several different online discussion forums, blogs and use other Web 2.0 media to market the product, answer user questions, understand user needs, gather bug reports, provide technical support and collaborate with vendors and other developers. The knowledge assets of the firm includes codified knowledge objects such as software toolkits and best practices as well as knowledge residing in its experts, development teams, and organizational units. Given that the firm's business model is heavily dependent on its knowledge assets, securing those knowledge assets, whether tacit or explicit, is a key requirement for the firm. In the rest of this section, we apply our proposed risk assessment framework and present an analysis of the knowledge sharing risks for the firm with respect to specific knowledge assets in particular collaboration settings. In order to illustrate key elements of our proposed framework in a concise manner, we focus only on a small subset of the knowledge assets and a single business process. The process illustrated here can be iteratively applied by considering multiple business processes and knowledge assets to perform a comprehensive analysis of the knowledge sharing risks at an organization.

The first step of the risk assessment process includes the identification of key business processes of the organization that involve the generation of new knowledge, utilization of organizational knowledge assets, and interaction with external entities. For example, consider the requirements analysis process in ABC Software's Rental Services Software Unit. The requirements gathering process includes the creation of new knowledge on market needs, application of industry specific best practices and templates for the collection of customer requirements, and involves interaction with customers and sub-contractors to gather requirements and analyze product offerings. A description of the process, entities involved and related knowledge assets is shown in Table 3.

Table 3 Key processes and entities involved

Process	Entities		Knowledge assets
	Internal	External	
Requirements analysis	Companies employees	Customers Sub-contractors	Employee1: Software consultant with expertise in rental industry Generic requirements analysis template Rental industry requirements elicitation best practice

The second step of the risk assessment process requires the manager to identify all the knowledge assets used in this process and to value the knowledge assets in terms of the competitive advantage derived by the organization through the assets. The knowledge assets are rated in terms of three criteria that include value, imitability, and uniqueness. Table 4 illustrates a sample rating of value, uniqueness and imitability for the knowledge assets identified earlier in the process. For example, while a generic requirements collection process is of significant value to conducting a business process, it is a widely used process across the industry and easily available. However, the retail industry specific best practices, and the tacit knowledge of a software consultant represent significant intellectual capital which is difficult to imitate and not widely available in the marketplace. Based on the ratings, the knowledge assets can then be ranked in terms of their strategic value using AHP-based multi-criteria decision algorithm to identify the most strategic knowledge assets. The project manager can then focus the risk management efforts on the strategically most important assets as identified by the ranking.

Table 4 Knowledge assets valuation

Knowledge asset	Value	Imitability	Rareness
Generic requirements collection template	3	1	1
Rental industry requirements collection template	4	2	3
Software consultant: rental industry	4	3	3

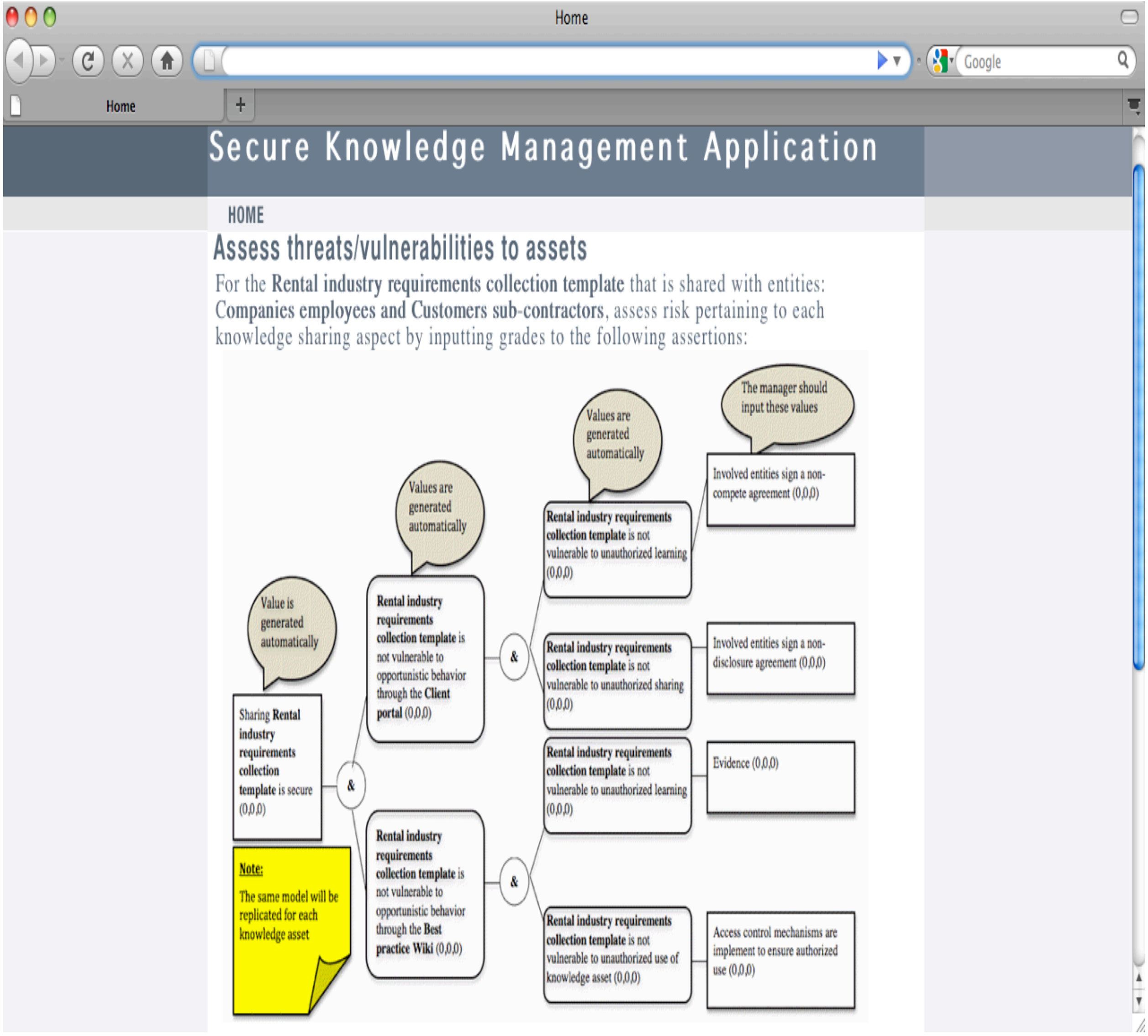
Following the identification of strategic knowledge assets, the next step would be to identify collaboration technology through which these assets are shared. The rental industry specific requirements collection best practices, for instance, which ranked high on value and rareness, is shared via Wiki's, Email, client portals and collaborative development environments with sub contractors. The knowledge assets and a list of collaboration technologies that expose the knowledge assets are given in Table 5.

Table 5 Identify collaboration technology

Knowledge asset	Context	
	Business process	**Technology**
Rental industry requirements collection template	Requirements analysis	Best practice Wiki Client portal Collaborative development environment Word forms over e-mail
Software consultant with rental industry experience	Requirements analysis	Best practice Wiki Corporate employee blogs

Once the technology through which strategic knowledge assets are shared is identified, the next step involves mapping the knowledge assets to potential threats and developing assertions that can be evaluated using an evidential reasoning model. There are several potential risks due to knowledge sharing as identified in Section 3.2. For example, a sub-contractor could engage in unauthorized learning and use of the best practice knowledge asset for developing competing products, or a client could share the requirements knowledge with a competing third party for development.

In order to develop a comprehensive understanding of the knowledge sharing risk, assertions regarding the knowledge assets and the threats are generated by mapping the different risks to knowledge assets in the context of various information and communication technologies that are used to share the knowledge assets. For example, a main assertion in this case states that the rental industry requirements elicitation best practice is not vulnerable to opportunistic behavior via an Extranet Knowledge Wiki. Sub-assertions would then break down this risk further to various threats such as manipulation, appropriation and other threats identified earlier. The assertions are then compiled into an evidential reasoning model as shown in Figure 7.



Secure Knowledge Management Application

HOME

Assess threats/vulnerabilities to assets

For the **Rental industry requirements collection template** that is shared with entities: **Companies employees and Customers sub-contractors**, assess risk pertaining to each knowledge sharing aspect by inputting grades to the following assertions:

Value is generated automatically
Values are generated automatically
Values are generated automatically
The manager should input these values
&
&
&

Sharing **Rental industry requirements collection template** is secure (0,0,0)

Note: The same model will be replicated for each knowledge asset

Rental industry requirements collection template is not vulnerable to opportunistic behavior through the **Client portal** (0,0,0)

Rental industry requirements collection template is not vulnerable to opportunistic behavior through the **Best practice Wiki** (0,0,0)

Rental industry requirements collection template is not vulnerable to unauthorized learning (0,0,0)

Rental industry requirements collection template is not vulnerable to unauthorized sharing (0,0,0)

Rental industry requirements collection template is not vulnerable to unauthorized learning (0,0,0)

Rental industry requirements collection template is not vulnerable to unauthorized use of knowledge asset (0,0,0)

Involved entities sign a non-compete agreement (0,0,0)

Involved entities sign a non-disclosure agreement (0,0,0)

Evidence (0,0,0)

Access control mechanisms are implement to ensure authorized use (0,0,0)

Figure 7 Mapping risks to knowledge assets, making assertions, and providing evidence

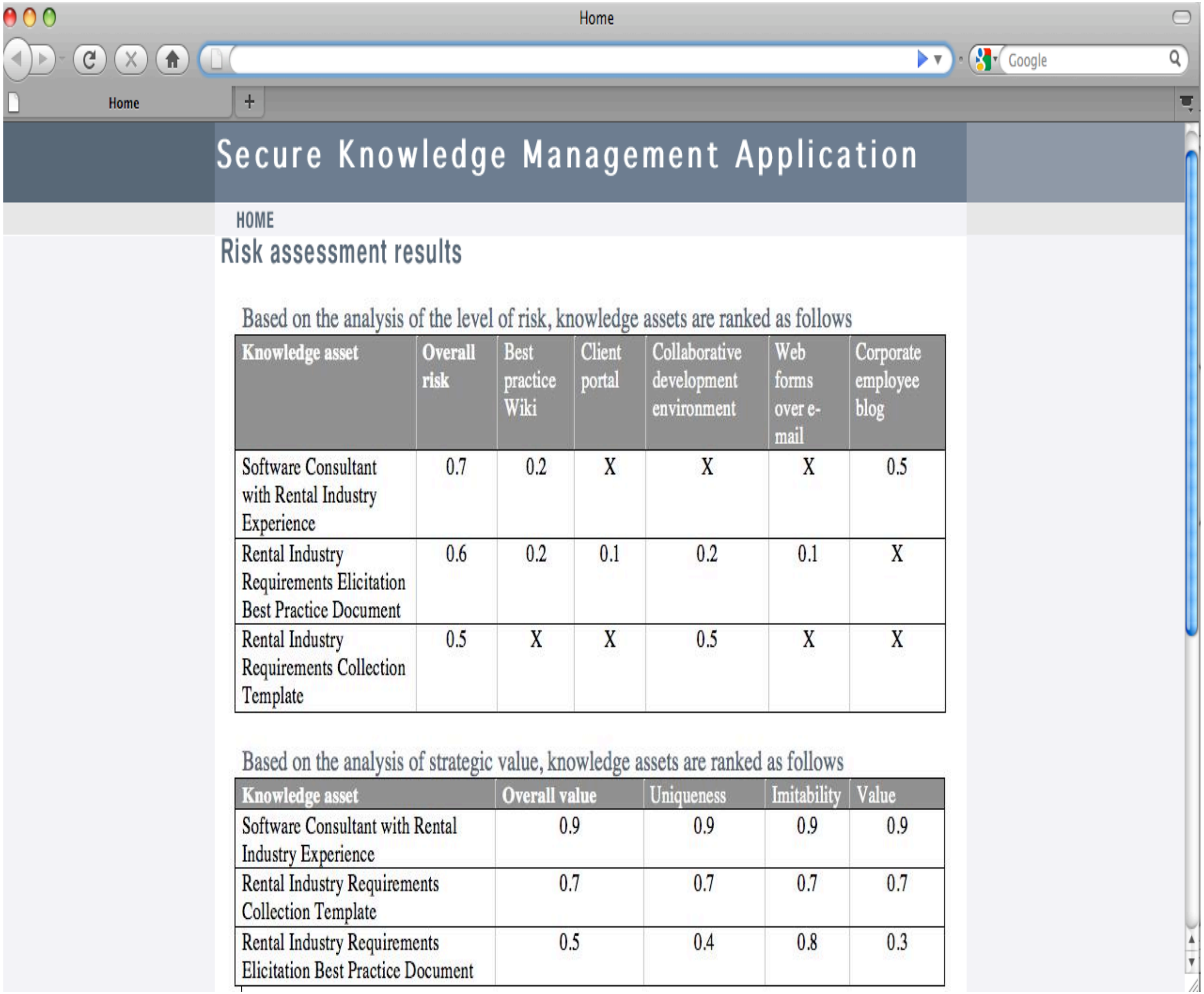
Following the mapping of threats to knowledge assets, the mitigation measures currently in place to protect the knowledge assets are evaluated to determine the residual risk. In this step the manager provides evidence, such as risk control mechanisms, to assess the extent to which knowledge assets are not vulnerable to various risks. For example, a manager may believe that sharing requirements elicitation best practice via the WIKI is not vulnerable to manipulation due to access controls mechanisms in place to prevent unauthorized changes. Similarly, the manager may believe that that non-disclosure agreement as a control mechanism is sufficient to mitigate unauthorized sharing risk. Examples of more measures to mitigate knowledge sharing risks are listed in Table 6.

Table 6 Mitigating measures

Measure
Use of Non-disclosure Agreements
Use of Non-compete Agreements

Access Control Mechanisms
Audit Trails/Traceability Mechanisms

In addition to providing the evidence, the manager also provides subjective estimates on the extent to which such measures mitigate the threats. For example, the estimates on the extent to which sharing best practices via a Wiki is not vulnerable to unauthorized sharing due to the use of non disclosure agreements is recorded as (0.7, 0.1, 0.2). Here 0.7 refers to the manager's belief on a 0-1 scale that non disclosure agreements prevent unauthorized sharing of the knowledge assets., whereas 0.1 refers to the the manager belief that non disclosure agreements are not effective in preventing unauthorized sharing and 0.2 refers to the degree of uncertainty of its effect on unauthorized sharing. Based on the estimates provided by the manager, the level of risk associated with each knowledge asset via a particular technology is calculated and displayed in a ranked order. In order to concentrate the manager's efforts on those assets that require the highest level of attention, the assets would be ranked based on their strategic value as can be noted from Figure 8. The manager can then determine additional security measures to protect the most strategic knowledge assets.



Secure Knowledge Management Application

HOME

Risk assessment results

Based on the analysis of the level of risk, knowledge assets are ranked as follows

Knowledge asset	Overall risk	Best practice Wiki	Client portal	Collaborative development environment	Web forms over e-mail	Corporate employee blog
Software Consultant with Rental Industry Experience	0.7	0.2	X	X	X	0.5
Rental Industry Requirements Elicitation Best Practice Document	0.6	0.2	0.1	0.2	0.1	X
Rental Industry Requirements Collection Template	0.5	X	X	0.5	X	X

Based on the analysis of strategic value, knowledge assets are ranked as follows

Knowledge asset	Overall value	Uniqueness	Imitability	Value
Software Consultant with Rental Industry Experience	0.9	0.9	0.9	0.9
Rental Industry Requirements Collection Template	0.7	0.7	0.7	0.7
Rental Industry Requirements Elicitation Best Practice Document	0.5	0.4	0.8	0.3

Figure 8 Calculating risks and ranking strategic assets

7. CONCLUSIONS

A critical dilemma that modern firms face in today's dynamic business environments is realizing the benefits of collaboration while maintaining competitive advantage, especially when collaboration involves sharing knowledge assets contributing to the firm's advantage. Incidents such as Intellectual Property (IP) leakage and failure of strategic alliances call for more research in this domain. While there is always a margin of error in predicting the success of inter-organizational relationships, organizations could benefit by following a more proactive approach in identifying potential vulnerabilities to strategic knowledge assets that are exposed in collaborative settings, which can help in the design of more efficient and dynamic securing policies.

In this paper, we have leveraged work in two relevant areas, knowledge management and risk assessment, in solving such a dilemma. Specifically, our contributions in this paper include (1) a risk assessment framework that assists project managers in identifying strategic knowledge assets that are shared through particular business processes using specific collaboration technologies. (2) a system design for a decision support system for knowledge sharing risks based on the proposed framework, and (3) an illustrative scenario that demonstrates the use and feasibility of our knowledge sharing risk assessment approach.

To the best of our knowledge, our approach is among the first to present a structured framework for organizations to help identify strategic knowledge assets and their vulnerabilities. The knowledge sharing risk assessment framework can provide significant benefits to organizations in identifying and protecting their strategic knowledge assets and competitive advantage.

REFERENCES

[1] R.Y. Arakji, K.R. Lang, Digital consumer networks and producer–consumer collaboration: Innovation and product development in the video game industry, Journal of Management Information Systems, 24(2) (2007) 195-219.

[2] F. Bayer, R. Maier, Knowledge risks in inter-organizational knowledge transfer, Proceedings of the 6th International Conference on Knowledge Management, Austria, September 6-8, 2006

[3] I. Becerra-Fernandez, A. Gonzalez, R. Shabherwal, Knowledge management and KM software packages, Prentice Hall, New Jersey, 2004.

[4] M. Beeby, C. Booth, Networks and inter-organizational learning: a critical review, The Learning Organization, 7(2) (2000) 75-88.

[5] F. Behrend, Collaborate today, compete tomorrow, Knowledge Management Review, 6(5) (2006) 24-27.

[6] B.A. Burrows, A little less swagger at Cisco, Business Week, http://www.businessweek.com/technology/content/nov2004/tc20041110_9788_tc024.htm, (November 10, 2004)

[7] S. Carlsson, Strategic knowledge managing within the context of networks, in: Handbook on Knowledge Management: Knowledge Matters, Springer-Verlag, New York, 2003.

[8] The OCTAVE approach, CERT Coordination Center, http://www.cert.org/, 2003

[9] Information Technology Infrastructure Library ITIL, The Office of Governement Commerce, http://www.itil-officialsite.com, 2001

[10] S.Cooper, Making sense of Web 2.0, Small Business Edge,

http://www.smallbusinessedge.com/article/Technology/Making_Sense_of_Web_2.0_, (June, 2009)

[11] T.K. Das, B. Teng, Trust, control, and risk in strategic alliances: An integrated framework, Organization Studies, 22(2) (2001) 251-284.

[12] T.K. Das, B.S. Teng, Managing risks in strategic alliances, The Academy of Management 13(4) (1999).

[13] A.P. Dempster, A Generalization of the Baysian Inference, Journal of Royal Statistical Society, 30(1968) 205-447.

[14] S. Dynes, H. Brechbühl, E. Johnson. Information security in the extended enterprise: Some initial results from a field study of an industrial firm, Proceedings of Workshop on the Economics of Information Security WEIS05, Boston, MA, June 2-3, 2005

[15] S. Dynes, L. Kolbe, R. Schierholz, Information security in the extended enterprise: A research agenda, Proceedings of the 13th Americas Conference on Information Systems AMCIS07, Denver, Colorado, August 9-12, 2007

[16] E. Fanning, Editor's Note: Security for Web 2.0, Computer World, http://www.computerworld.com/s/article/283283/Security_for_Web_2.0, (March 19, 2007)

[17] F. Farahmand, S. Navathe, G. Sharp, P. Enslow, Proceedings of Managing vulnerabilities of information systems to security incidents, Proceedings of the 5th International Conference on Electronic Commerce, Pittsburgh, Pennsylvania, September 30-October 3, 2003

[18] F. Farahmand, G. Sharp, P. Enslow, A management perspective on security threats to information systems, Information Technology and Management, 6 (2005) 203-225.

[19] R. Freeze, U. Kulkarni, Knowledge management capability assessment: Validating a knowledge assets measurement instrument, Proceedings of the 38th Hawaii International Conference on Systems Sciences, Waikoloa, Hawaii, January 3-6 2005

[20] S. Goto, The bounds of classical risk management and the importance of a behavioral approach, Risk Management and Insurance Review, 10(2) (2007).

[21] S. Hamm, IBM Takes on Amazon, Business Week, http://www.businessweek.com/technology/content/oct2006/tc20061023_158174.htm?chan=top+news_top+news+index_businessweek+exclusives, (October 23, 2006)

[22] C. Hardy, N. Phillips, T.B. Lawrence, Resources, knowledge and influence: The organizational effects of inter-organizational collaboration, Journal of Management Studies, 40(2) (2003).

[23] A. Hargadon, R. Sutton, Building Innovation Factory, Harvard Business Review, (2000) 157-166.

[24] M. Herbst, Satyam's U.S clients face tough choices, Business Week, http://www.businessweek.com/bwdaily/dnflash/content/jan2009/db2009019_127597.htm?chan=technology_technology%20index%20page_computers, (January 9, 2009)

[25] C. Hilhorst, P. Ribbers, E. Heck, M. Smits, Using the Dempster-Shafer theory and real options to assess competing strategies for implementing IT insfrastructures: A case study, Decision Support Systems, 46(2008) 344-355.

[26] COBIT, IT Governance Institute, http://www.ITgovernance.org, 2001

[27] E. Johnson, S. Dynes, Inadvertent disclosure: Information leaks in the extended enterprise, Proceedings of the 6th Workshop on the Economics of Information Security, Pittsburgh, PA, June 7-8, 2007

[28] M. Levy, P. Powell, SMEs, co-opetition and Knowledge Sharing: The Role of Information Systems, European Journal of Information Systems, 12(2003) 3-17.

[29] R.S. Marshall, T. Nguyen, S.E. Bryant, A dynamic model for trust development and knowledge sharing in strategic alliances, Journal of General Management, 31(1) (2005) 41-57.

[30] J.W. Medcof, Why too many alliances end in divorce, Long Range Planning, 30(5) (1997).

[31] G. Mentzas, D. Apostolou, K. Kafentzis, P. Georgolios, Inter-organizational networks for knowledge sharing and trading, Information Technology Management, 7(4) (2006) 259-276.

[32] R. Oricchio, Web 2.0 brings increased array of threats, Cio Strategy Center, http://www.ciostrategycenter.com/ktvt/Threat/preparedness/increased_web_threats/index.html (September, 2009)

[33] N. Panteli, S. Sockalingam, Trust and conflict within virtual inter-organizational alliances: a framework for facilitating knowledge sharing, Decision Support Systems, 39(4) (2005) 599-617.

[34] A.T. Pardo, A. Cresswell, T.F. Zhang, Knowledge sharing in cross-boundary information system development in the public sector, Information Technology Management, 7(2007) 293-313.

[35] M. Probasco, Workers flood blogs with company secrets, http://www.newser.com/story/64791/workers-flood-blogs-with-company-secrets.html, (July 20, 2009)

[36] J. Rees, S. Bandyopadhyay, E. Spafford, PFIRES: A policy framework for information security, Communications of the ACM, 46(7) (2003).

[37] T. Saaty, Decision Making with the analytic hierarchy process, International Journal of Services Sciences, 1(1) (2008) 83-89.

[38] B. Schlaak, S. Dynes, L. Kolbe, R. Schierholz, Managing of information systems risks in extended enterprises-The case of outsourcing, Proceedings of the 14th Americas Conference on Information Systems, Toronto, Canada, August 14-17, 2008

[39] G. Shafer, A Mathematical Theory of Evidence, Princeton University Press, Princeton, New Jersey, 1976.

[40] J. Short, Risks in a web 2.0 world, Risk Management, http://www.rmmagazine.com/MGTemplate.cfm?Section=RMMagazine&NavMenuID=128&template=/Magazine/DisplayMagazines.cfm&IssueID=328&AID=3760&Volume=55&ShowArticle=1, (June, 2009)

[41] T. Spring, Work for a big company? odds are good your boss is reading your e-mail: study, PC World, http://blogs.pcworld.com/staffblog/archives/007005.html, (May 23, 2008)

[42] The Information Security Management Systems Family of Standards, The International Organization for Standardization, http://www.iso.org/, 2000

[43] G. Stoneburner, A. Goguen, A. Feringa, Risk Management guide for information technology Systems: Recommendations of the National Institute of Standards and Technology, NIST, csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, 2001

[44] L. Sun, R. Srivastava, T. Mock, An Information Systems Security Risk Assessment Model under the Dempster-Shafer Theory of Belief Functions, Journal of Management Information Systems, 22(4) (2006) 109-142.

[45] S. Sutton, C. Hampton, D. Khazanchi, V. Arnold, Risk analysis in extended enterprise environments: identification of critical risk factors in B2B e-Commerce relationships, Journal of the Association of Information Systems, 9(3/4) (2008).

[46] C. Zhang, S. Li, Secure Information Sharing in Internet-Based Supply Chain Management Systems, Journal of Computer Information Systems, 46(4) (2006) 18-24.

[47] J. Zhen, The War on Leaked Intellectual Property, Computer World, http://www.computerworld.com/s/article/98724/The_war_on_leaked_intellectual_property, (January 5, 2005)

芽|Sprouts

Working Papers on Information Systems | ISSN 1535-6078

Office:
Sprouts
University of Amsterdam
Roetersstraat 11, Room E 2.74
1018 WB Amsterdam, Netherlands
Email: admin@sprouts.aisnet.org