Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2009 Proceedings

Americas Conference on Information Systems (AMCIS)

2009

A Framework for Assessing Knowledge Sharing Risks in Interorganizational Networks

Ruba Aljafari
Dakota State University, raljafari@unomaha.edu

Surendra Sarnikar
Dakota State University, ssarnikar@outlook.com

Recommended Citation

Aljafari, Ruba and Sarnikar, Surendra, "A Framework for Assessing Knowledge Sharing Risks in Interorganizational Networks" (2009). *AMCIS 2009 Proceedings*. 572.
http://aisel.aisnet.org/amcis2009/572

A Framework for Assessing Knowledge Sharing Risks in Inter-Organizational Networks

Ruba Aljafari
Dakota State University
rhaljafari@pluto.dsu.edu

Surendra Sarnikar
Dakota State University
Surendra.sarnikar@dsu.edu

ABSTRACT

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 that can be exposed through collaboration technologies, and help prioritize security strategies that can be used to secure the collaboration systems to prevent the loss of valuable knowledge assets. We present an illustrative case to demonstrate the feasibility of the framework, and discuss issues for future research.

KEYWORDS

Knowledge sharing, Collaboration, Risk assessment.

INTRODUCTION

Organizations are increasingly using collaboration technologies and systems to move towards collaborative inter-organizational network structures. Such network structure are being use to manage various business processes such as supply chains processes, joint product development, customer relationship management., developing industry standards, and engaging in collaborative commerce. In addition to formalized inter-organizational collaboration mechanisms, knowledge workers are also using web-based collaboration technologies such as Wiki's, blogs, discussion forums, social networks and online communities to engage in ad hoc collaboration with customers and vendors to exchange knowledge and provide improved services. While such inter-organizational collaboration has many benefits, risks pertaining to knowledge sharing may arise when knowledge, for example, is transferred to other projects that may benefit competitors. Several news reports and companies such as IBM, Cisco reported cases of intellectual property leakage and loss due to insufficient protection of knowledge assets (Zhen, 2005; Herbst, 2009; Hamm, 2006; Burrows, 2004).

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 been done in the area of information security risk assessment and security mechanisms for inter-organizational collaboration systems. However, their focus is limited to technology infrastructure and data and information assets and do not consider knowledge assets. There is limited literature that helps identify 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. The term risk is used in this study to refer to the potential damage, loss, or negative effect of knowledge sharing.

In this paper, we build on past research in knowledge sharing, secure collaboration systems, and Information Systems risk assessment, to propose a preliminary framework for identifying knowledge assets exposed by collaboration systems and a mechanism for valuing and securing the exposed knowledge assets. The proposed framework will help organizations systematically indentify risks of knowledge sharing and how they can mitigate risks arising due to participants in collaborative environment. The proposed framework consists of four specific components that focus on (1) identifying knowledge assets, (2) identifying collaboration technologies that expose the knowledge assets, (3) identifying the risk associated with the knowledge assets, and (4) a Dempster-Shaefer based model for quantifying the risks.

The rest of the paper is organized as follows: The next section provides background and context on inter-organizational collaboration. The following section reviews relevant literature in the areas of knowledge sharing and risk assessment methodologies. Then we present the foundations of the proposed risk assessment model, followed by an illustrative case. And the final section concludes with a summary of contributions and issues for future research.

BACKGROUND

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 (Hargadon and Sutton, 2000). Organizations are therefore increasingly exploring inter-organizational knowledge sharing arrangements within an environment that allows them to build valuable intellectual capital and knowledge assets (Hardy, Phillips, and Lawrence, 2003)

It is important to note that although inter-organizational networks may involve sharing data such as inventory levels, information such as sales figures, and knowledge such as best practices, our focus will be only on knowledge. Based on the hierarchical view of data, information, and knowledge as discussed by Alavi and Leinder (2001), we define knowledge as processed information. Typical knowledge sharing scenarios in an inter-organization network are presented in Figure 1 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 change 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. For example, computer engineers and knowledge workers at the computer manufacturer 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.

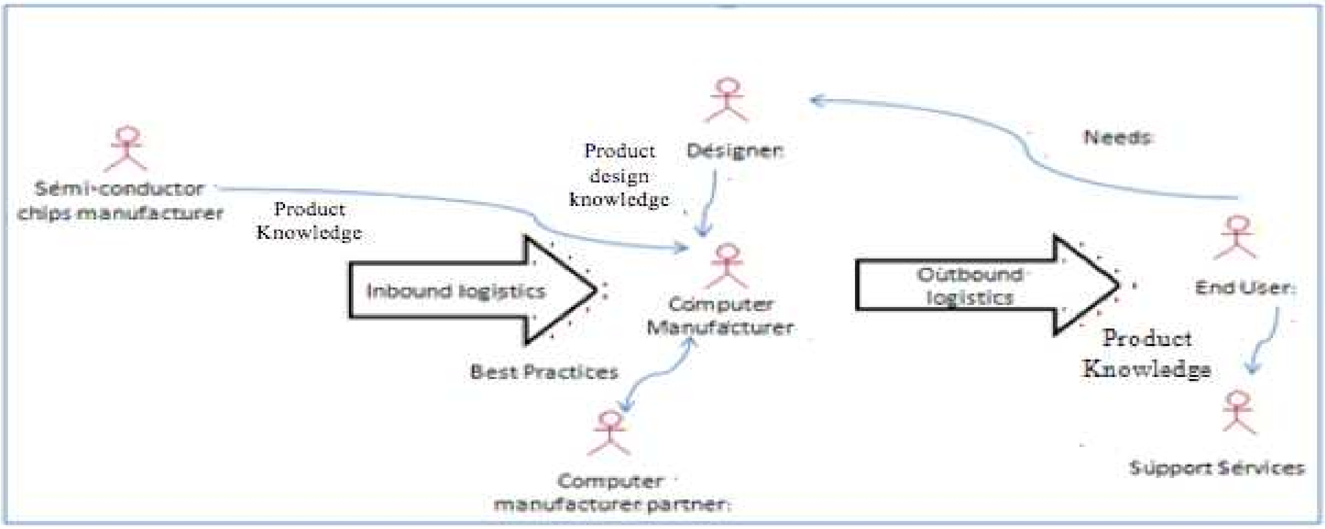

Figure 1. Knowledge Sharing in the Computer Industry

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 (Marshall, Nguyen, and Bryant, 2005). 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 to the firm that owns the original product or when the partner decides to move to innovating the basic product (Arakji and Lang, 2007).

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.

LITERATURE REVIEW

In this section we present a review of literature in inter-organizational knowledge sharing and information security and risk analysis that form the foundation of our research.

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, while the behavioral perspective includes research that explores behavioral issues related to collaborative knowledge sharing, for example: trust and social ties among participants in the same collaborative system.

The third perspective investigates inter-organizational knowledge sharing from a strategic perspective. This perspective is the closest to our study. In order to analyze the strategic impact of knowledge sharing, Levy, Leobbecke, and Powell (2003) proposed a game theoretic approach to analyze inter-organizational knowledge sharing among SMEs. To control knowledge sharing on the organizational level, most firms depend on legal contracts and policies that govern areas of knowledge exchange. Developing these procedures that should ensure high level of control and flexibility at the same time could be complex, as explained by Behrend (2006), organizations may use the acquired knowledge beyond boundaries of legal agreements describing the knowledge assets to be exchanged, so protecting the key know-how is critical.

Knowledge sharing may be beneficial in learning, specifically in strategic alliances. According to Medcof (1997), partners can learn from each other business and management skills that they were lacking individually. A more strategic view suggests that knowledge sharing enables the creation of new knowledge and synergistic solutions (Hardy et al. 2003).

Knowledge sharing can also play an important role in solving problems. In the supply chain domain, for instance, benefits of information sharing were widely discussed as solutions to overcome problems associated with supply chain integration. For example, Croson and Donohue (2006) examined how sharing points of sales data (POS) can reduce the bullwhip effect, which is a phenomenon that appears in the supply chain where variability in demand increases as we go to the upstream of the supply chain (Levi, 2003). To solve this problem, most researchers emphasized that coordination, through sharing information, among manufacturers, wholesalers, distributors, and retailers can reduce this variability (Lin, Wu, Hung, Lin, 2002).

Previously discussed benefits should be weighed against risks pertaining to knowledge sharing. Such risks may include diffusion of the firm's knowledge (Beeby and Booth, 2000) as the value of the shared knowledge diminishes, which may result in the loss of competitive advantage (Pardo, Cresswell, Thompson, and Zhang, 2007).. In strategic alliances, predicting and managing conflicts, which may be important sources of risk, is usually overlooked (Panteli and Sockalingam, 2005). According to Das and Teng (2001), there can be two types of risks in strategic alliances: relational risk and performance risk. Relational risk may arise 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 Das and Teng (2001), 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 (Zhang and Li, 2006). Performance risk is basically related to the probability that alliance objectives may not be met despite good relations between partners (Das and Teng, 2001) such risk may arise because of new entrants to the industry, demand fluctuations, changing government policies, and lack of competence of partner firms. Table 1. summarizes types of the benefits and risks associated with knowledge sharing.

Benefits	Risks
Knowledge acquisition	Knowledge diffusion
Synergistic opportunities	Opportunistic behavior
Solving problems	Performance problems

Table 1. Types of Knowledge Sharing Risks and Benefits

Knowledge sharing risks are not explicitly and widely discussed in the literature. Risks and benefits of knowledge sharing identified in the literature depend on the perspective taken to analyze knowledge sharing. For example, if that perspective was technical, risks can arise from unauthorized access to knowledge resources. This study will rely to a great extent on the results of the studies mentioned in the strategic perspective to identify knowledge-sharing risks that will be used later in the risk assessment model.

Risk Assessment

A significant amount of literature exists in the IT/IS risk assessment domain in general and risk assessment within inter-organizational business networks in specific. The main focus of the risk assessment literature in the IS/IT is securing IT assets from external and internal threats. On the other hand, risk assessment in inter-organizational business networks analyzes the effects of business relations and collaboration.

There are several IT risk assessment models proposed in literature. A typical risk assessment process begins with identifying data, information and technology assets that might be exposed to risk, and quantifying threats associated with them (Rees, Bandyopadhyay, and Spafford, 2003). This process can be challenging since evaluation in this domain can be highly subjective (Farahmand, Navathe, Sharp, and Enslow, 2003). After identifying those vulnerable assets and determining risk, experts can design and then select and apply the best protection mechanisms then evaluate them in an iterative manner. (Farahmand et al. 2003; Farahmand, Sharp, and Enslow, 2005) Most of risk assessment models resemble the previously discussed logic. Examples of such models include: The Policy Framework for Interpreting Risk in E-business Security (PFIRES) designed by Rees et al. (2003), The Risk Management Guide for Information Technology Systems by (Stoneburner, Goguen, and Feringa, 2001), OCTAVE (Cert coordination center, 2003), and COBIT (IT governance institute, 2001). Our proposed framework resembles the logic of these models as well, especially the preliminary phases used to identify assets and quantify risks.

In addition to IT risk assessment models, another group of work that examines risk assessment techniques is relevant to our work. Zsidisin, Ellram, Carter, and Cavinato (2004) reviewed and evaluated different risk assessment frameworks within inbound supply chains. They analyzed the effect of using risk assessment processes including risks arising from the nature of relationships among participants such as goal conflict in a business relationship. In their proposal of a web-based risk assessment tool for distributed construction teams, Shang, Anumba, Bouchlaghem, Miles, Cen, and Taylor (2005) found that the use of this system offers flexibility and greater consistency among teams. Although knowledge sharing risks were not explicitly identified, complexity of relationships in such collaborative projects was addressed. In their analysis of the effect of information sharing on profitability, Kulp, Lee, and Ofek (2004)) highlighted the fact that information sharing should reduce, for instance, stock-out occurrence, also coordinate design, development, and introduction of new products. Such findings can be helpful for firms assessing effects of engaging into collaboration, and therefore, weight benefits against costs. Such analysis can be very useful in highlighting those risks arising from the nature of the relationship.

While there are risk assessment frameworks for information security in specific business relationships such as the supply chains, there is no framework that can help analyze risks in inter-organizational knowledge sharing. Organization's knowledge assets, which may be tacit or explicit, are vulnerable to threats when exposed to external organizations in the process of strategic, operational, formalized, or ad hoc collaboration arrangements. For example, in the context of collaborative product development, is there a risk that the firm's partners acquire competencies that the sharing firm contributes to the product development? Is there a risk that those partners gain access to knowledge that the sharing firm uses in other business areas (Parker, 2000)? 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 the above scenarios. In the next section, we build on past literature in risk assessment to develop a framework that can help in assessing risks of knowledge sharing, since knowledge can be derived from information and is often shared using information and communication technologies. However, knowledge loss and distortion can cost the firm greater losses since it takes years and more resources to develop knowledge, whether it was explicit or tacit.

RISK ASSESSMENT MODEL

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 (Stoneburner et al. 2001), and PFIRES by Rees et al. (2003), to develop a risk assessment framework that is suited for the inter-organizational knowledge sharing case. As mentioned previously, preliminary phases in our framework resemble those in NIST and PFIRES but are modified to incorporate knowledge characteristics. The following discussion presents main steps in this model and the purpose, method, and output in each step:

Identify Knowledge Assets

According to Freeze and Kulkarni (2005), knowledge assets are "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". So managers can identify and classify these assets as a start. This is important because being specific about the knowledge type can assist in identifying those threats and later identifying securing policy.

Objective: To identify knowledge assets that need to be protected

- Organizational knowledge assets may reside in people, documents etc. One approach that can be used to identify these assets is to sketch a tree diagram with different types of knowledge resources, so that managers can clearly spot and identify knowledge assets.

Method

- Start by locating knowledge assets. One useful way is to apply the knowledge reservoirs graph designed by Becerra-Fernandez, Gonzalez, and Shabherwal (2004) as can be noted from Figure 2. Knowledge can be stored in one individual's or expert's mind as tacit knowledge or in groups as collective and synergistic (Becerra-Fernandez et al., 2004). It can also be encapsulated in artifacts such practices (e.g. procedures and rules), technologies, and knowledge repositories. Another approach that can be applied is to use the set of measures of Knowledge Capability Areas (KCA) proposed by Freeze and Kulkarni (2005). These measures include lessons learned, knowledge documents or codified knowledge, expertise, and data.

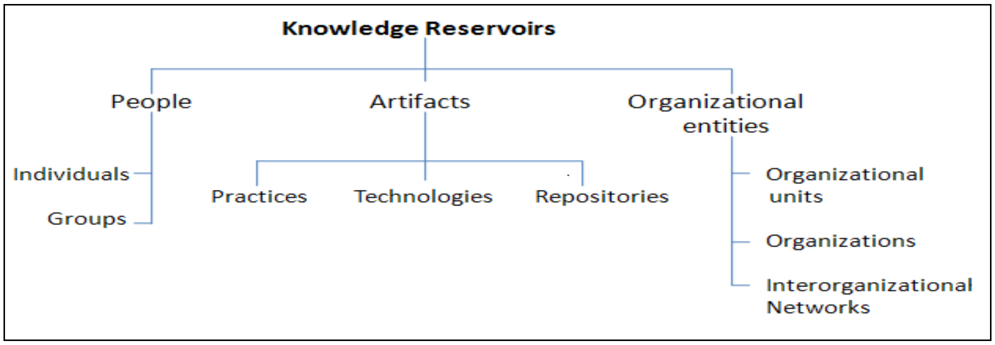

Figure 2. The Reservoirs of Knowledge (Adapted from Becerra-Fernandez et al., 2004)

- Identify strategic knowledge assets by assessing their (1) value, (2) rareness and (3) 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 (Carlsson, 2003). A knowledge resource is strategically important to an organization based on characteristics such as: 1) Value: Does the knowledge enable the firm to sense and respond to opportunities and threats in the business environment. 2) Rareness: To what extend do competing firms possess similar knowledge, and 3) Imitability: Is the knowledge resource costly and difficult to acquire for other organizations that do not own it to obtain or imitate

Output: A list of strategic knowledge assets and their characteristics

Identify Inter-organizational Knowledge Sharing Practices

Objective: Identify business processes in general and any possible ad hoc situations in which knowledge assets are used and exchanged

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
- Map previously identified knowledge assets to the business processes

Output: A list of business processes, related knowledge assets and inter-organizational knowledge sharing activities

This step is based on the notion that boundaries of the IT system must be defined in early stages of assessment (Stoneburner et al., 2001). In the context of this study, an organization should first define the scope of knowledge sharing process by identifying the business process, related knowledge assets and the activities in those processes that interface with external entities.

Identify Collaboration Technologies

Objective: To identify the medium or collaboration technology through which knowledge is transferred among business processes.

Method

- Identify technologies used in the context of previously identified processes. For example, a collaboration technology might be discussion boards, WIKI's, blogs…etc. This step leads to identifying vulnerabilities.

Output: Develop a Process-Technology-Asset matrix to document the knowledge asset vulnerabilities.

.

Identify Vulnerabilities and Threats to Knowledge Assets

Objective: Identify threats and vulnerabilities to knowledge assets
Method:

- List potential threats and vulnerabilities to knowledge assets. Vulnerability is defined by Stoneburner et al. (2001), as "A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised and result in a security breach or violation of the system's security policy". If two teams, for instance, are sharing best practices via online blogs, what kinds of vulnerabilities are there? Vulnerabilities can emerge from the technology itself, such as: unauthorized access to knowledge repositories or through the inadvertent release of strategic knowledge. Threats arising due to knowledge sharing include knowledge diffusion, opportunistic behavior and performance risk. Vulnerabilities may also arise from ad hoc collaboration. A manager may, for instance, monitor discussion forums to identify any incident of negative knowledge transfer.
- Identify which of the above identified vulnerabilities apply to the knowledge assets under consideration

Output: List of applicable threats and vulnerabilities

Make Assertions

Objective: Based on knowledge asset value, ease of transfer, and potential transfer mechanisms (Vulnerabilities, collaboration technologies), make assertions on knowledge asset vulnerabilities

Method:

1. Map knowledge assets to vulnerabilities
2. For each mapping list, value of knowledge asset, ease of transfer, potential transfer mechanism
3. Make assertions, as called by the Dempster-Shafer theory, on the vulnerability of knowledge asset through technology. For example: knowledge asset x is not vulnerable to diffusion through employee blogs. This can be based on the extent to which managers think that the shared knowledge will not be used beyond the collaboration agreement

Output: Assertions on knowledge asset vulnerabilities

Provide Evidence

Objective: Support previous assertions by evidence and estimate the likelihood of risk on these assertions

Method:

1. Expert judgment. Experts should support their assertions by evidence, which is assigned a specific value from 0-1 to measure its strength. . For example an expert might decide that in order to evaluate whether knowledge sharing is risk free or not, it is important to focus on whether the intellectual property of this shared knowledge is protected, then the manager can input his/her own judgment about this threat. More specifically, a manager can have a 0.4 belief that knowledge sharing is secure, a 0.10 belief that it is not secure, and a 0.50 level of ignorance indicating whether it is secure or not is unknown. 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 (Sun, Rajendra, and Theodore, 2006).
2. Calculate the plausibility that knowledge sharing is not secure, which is equal to 0.60, according to the numbers used in the previous step.

Output: Assertions and risk likelihood estimates from multiple experts

Calculate Risk

Objective: Calculate risk by integrating estimates from multiple experts
Method; Depmster-Shaefer model

Based on likelihood of transfer and the strategic value of knowledge asset, we use a Dempster-Shafer theory based model to calculate risks (Demspter, 1968; Shafer 1976). that 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 Baysian theory of subjective beliefs and is widely applied in diverse domains including information systems risk assessment (Sun et al., 2006).
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: Risk estimates

Develop Policy

After the overall level of risk is calculated, the firm needs to develop a security policy in order to mitigate these risks. More details about this step can be found in (Rees et al., 2003). One way, for example, is to focus on evaluating the reputation of the potential partners. As Bayer and Maier (2006) explained, this can help control opportunistic behavior.
Figure 3 summarizes the previous steps in the risk assessment process.

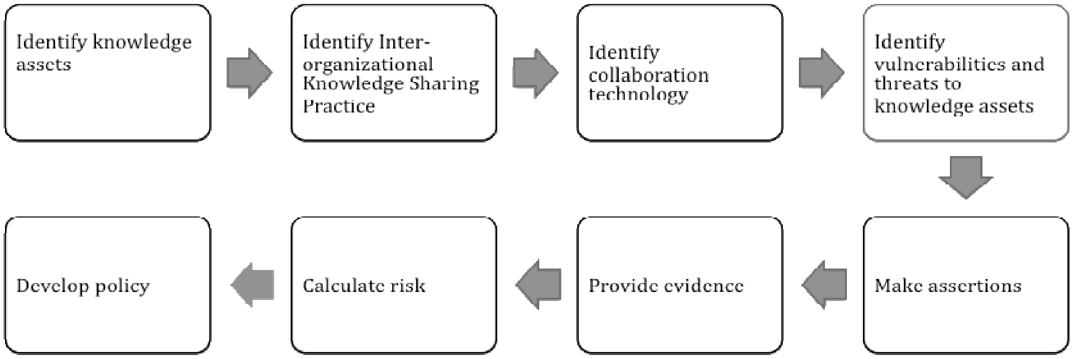
Identify knowledge assets
Identify Inter-organizational Knowledge Sharing Practice
Identify collaboration technology
Identify vulnerabilities and threats to knowledge assets
Make assertions
Provide evidence
Calculate risk
Develop policy

Figure 3: Risk assessment process

HYPOTHETICAL EXAMPLE

Suppose that a computer manufacturer, as can be noticed from Figure 1, is considering collaboration and wants to evaluate risks of sharing knowledge, such as best practices applied in the computer manufacturing process, with another computer manufacturer. Figure 4 shows this chosen scenario from Figure 1. Team A and Team B are engaged into knowledge sharing through different communication channels, using diverse technologies, and exchanging different types of knowledge. For example, developers from different teams can share programming knowledge through discussion forums and WIKI's

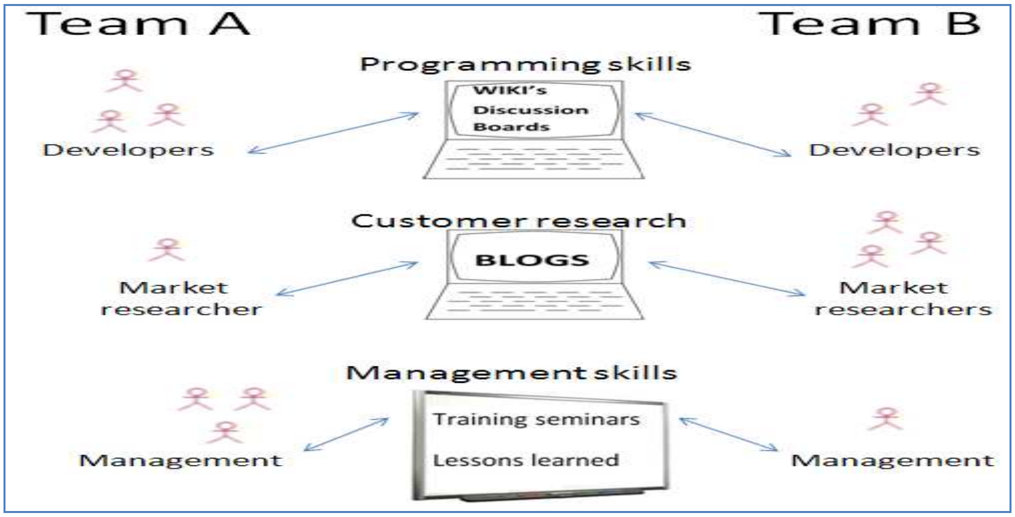

Figure 4. Knowledge Sharing Scenario

Managers will assess risks in this scenario through the following steps:

1. Identify knowledge assets: as illustrated in Figure 2, these assets include tacit assets such as programming and management skills and explicitly codified ones such as customer and market research. Then, they will ask questions of value and rareness (Carlsson, 2003). For example: How many competing firms own such knowledge.
2. Identify Inter-organizational Knowledge Sharing Practices: In this case, it will be the product development business process.
3. Identify collaboration technology. Sharing programming skills, for instance, makes use of Discussion boards and WIKI's.
4. Identify vulnerabilities and threats: Vulnerabilities that arise from the technology such as authentication and vulnerabilities that arise from people such as opportunistic behavior
5. Make assertions: managers with the help of experts start to form their assertions from the highest-level. This assertion states that sharing best practices knowledge through WIKI's has a positive effect on the sending party. If sharing best practices is risk free, it should be secure and synergistic, which represent the two sub-assertions of the main assertion. Figure 5 illustrates this model, which resembles the one used by Sun et al. (2006). According to Levy et al. (2003), knowledge sharing can be synergistic when both companies exchange knowledge and the company can yield additional value beyond the sum of companies' individual knowledge. They also stated that knowledge sharing can be synergistic mostly in manufacturing companies. The rounded box and the two ovals represent assertion nodes, the main one is numbered 1 and the sub-assertions are numbered 1.1 and 1.2.
6. Provide evidence: In order to support this assertion, evidence such as that sharing best practice can reduce cost, improve innovation, and coordination should be evaluated, again according to the beliefs of experts and managers. To evaluate whether sharing best practices is secure, companies will need to focus on evaluating the extent to which they think privacy is protected, for example: whether they have agreements that determine specific constraints to the use of WIKI's, and the extent to which they trust their partners. The rectangular boxes in Figure (5) represent evidence that support the main assertion and each of the sub assertions. The relationships between assertions, whether main assertion and sub-assertions and higher-level sub-assertions and lower level sub-assertions should be defined using logical relationships such as and/or (Sun et al., 2006).
7. Calculate risk: After identifying the evidence of assertions and the strength of the each evidence, the overall strength is computed to determine the level of risk.

8. Develop policy: If the situation analysis revealed unacceptable level of risk, which varies from a firm to another, experts will develop a policy to mitigate this risk. For example, if they think that there is not enough constraints on how knowledge is used via WIKI's or blogs, they would recommend changes to the collaboration agreements.

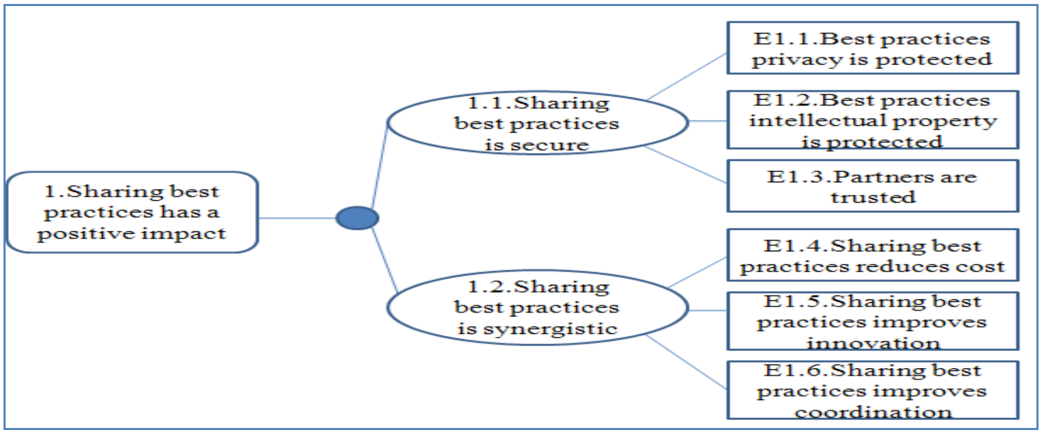
1.Sharing best practices has a positive impact
1.1.Sharing best practices is secure
1.2.Sharing best practices is synergistic
E1.1.Best practices privacy is protected
E1.2.Best practices intellectual property is protected
E1.3.Partners are trusted
E1.4.Sharing best practices reduces cost
E1.5.Sharing best practices improves innovation
E1.6.Sharing best practices improves coordination

Figure 5. Evaluating Evidence and Assertions

Table 2 summarizes steps and output in each one in this scenario.

№	Step	Output	
1	Identify knowledge assets	Type	Form
		Tacit or explicit	Best practices
2	Identify Inter-organizational Knowledge Sharing Practices	Product development	
3	Identify collaboration technology	WIKI's +Discussion boards	
4	Identify vulnerabilities	Authentication and opportunistic behavior	
5	Make assertions	Main	Sub
		1.Sharing best practices has a positive impact	1.1Sharing is secure
			1.2 Sharing best practices is synergistic
6	Provide Evidence	E1.1 Best practices privacy is protected	
		E1.2 Best practices intellectual property is protected	
		E1.3 Partners are trusted	
		E1.4 Sharing best practices reduces cost	
		E1.5 Sharing best practices improves innovation	
		E1.6 Sharing best practices improves coordination	
7	Calculate risk	Overall level of risk based on risk associated with evidence and sub-assertions	
8	Develop policy	Improve authentication Update knowledge sharing constraints in collaboration agreement	

Table 2. Summary of Risk Assessment Process

PROPOSED EVALUATION

In this paper, we have demonstrated the feasibility of the proposed framework using an illustrative case. However, the utility of framework can only be assessed through a field study that will be designed to measure, for example, manager's satisfaction with this framework. More specifically, whether this framework can improve the risk assessment process in evaluating collaborative agreements and the extent to which this framework help reduce subjectivity in risk assessment compared to old models used in this domain.

CONCLUSIONS, LIMITATIONS, AND FUTURE RESEARCH

Collaboration has attractive benefits that can lead organizations to overlook risks associated with it. Similar to information, knowledge is an important resource shared in such collaboration agreements. This paper proposes a risk assessment model that builds on information security risk assessment models to address the security of strategic knowledge assets. It is unique in the sense that it is specific to knowledge sharing among inter-organizational teams, and that it addresses subjectivity in evaluating risk associated with such type of collaboration by applying the logic of the Dempster-Shafer theory of beliefs. However, the framework has some limitations that we intend to address in a future field study to implement and evaluate the framework. The underlying processes, for instance, is resource intensive and requires considerable effort on part of the managers to identify and value knowledge assets. In order to address this limitation, we plan to develop a knowledge-based decision support system that will automate and support the decision making tasks. A second limitation is related to the need to identify and analyze ad hoc collaboration by knowledge workers. Although this issue is considered in step 2 of our proposed process, is not very well addressed. We intend to further investigate mechanisms for addressing this issue. Finally, the framework focuses mostly on IT-based vulnerabilities as most communication among individuals and organizations deploys some form of IT. Non-IT vulnerabilities, however, is yet another aspect to consider for future research.

REFERENCES

1. Alavi, M. and Leidner, D. (2001) Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues. MIS Quarterly, 25, 1, 107-136
2. Arakji, R. Y. and Lang, K. R. (2007) Digital Consumer Networks and Producer–Consumer Collaboration: Innovation and Product Development in the Video Game Industry. Journal of Management Information Systems, 24,2, 195-219.
3. Bayer F. and Maier R. (2006) Knowledge Risks in Inter-Organizational Knowledge Transfer. Proceedings of I-KNOW '06
4. Becerra-Fernandez I., Gonzalez A., Shabherwal R. (2004) Knowledge Management and KM Software Packages, Prentice Hall.
5. Beeby, M. and Booth, C. (2000) Networks and inter-organizational learning: a critical review, The Learning Organization, 7, 2, 75-88.
6. Behrend, F. (2006) Collaborate today, compete tomorrow. Knowledge Management Review, 6,5, 24-27.
7. Burrows, P. (2004) A Little Less Swagger at Cisco, Business Week, New York, Nov 10
8. Carlsson S.(2003) Strategic Knowledge Managing within the Context of Networks. In. Holsapple C W. eds. Handbook on Knowledge Management: Knowledge Matters [M], New York: Springer-Verlag.
9. CERT COORDINATION CENTER, 2003, The OCTAVE approach, http://www.cert.org/
10. Croson, R. and Donohue, K. (2006) Behavioral Causes of the Bullwhip Effect and the Observed Value of Inventory Information. Management Science, 52, 3, 323-336
11. Das T K. and Teng B. (2001) Trust, control, and risk in strategic alliances: An integrated framework, Organization Studies. Berlin, 22,2, 251-284
12. Dempster, A. P. (1968). A Generalization of the Baysian Inference. Journal of Royal Statistical Society, 30, 205-447
13. Farahmand, F., Navathe, S., Sharp, G., Enslow, P. (2003) Managing vulnerabilities of information systems to security incidents, Communications of the ACM.
14. Farahmand, F, Sharp, G., Enslow, P. (2005) A management perspective on security threats to information systems, Information Technology and Management, 6, 203-225
15. Freeze R. and Kulkarni U. (2005) Knowledge Management Capability Assessment: Validating a Knowledge Assets Measurement Instrument. Proceedings of the 38th Hawaii International Conference on Systems Sciences.
16. Hamm, S. (2006) IBM Takes on Amazon. Business Week, New York. Oct 24.
17. Hardy, C., Phillips, N., Lawrence, T. B. (2003) Resources, knowledge and influence: The organizational effects of inter-organizational collaboration. Journal of Management Studies, 40, 2.
18. Hargadon, A. and Sutton, R. (2000) Building Innovation Factory, Harvard Business Review (May-June), 157-166.

19. Herbst, M. (2009) Satyam's U.S Clients Face Tough Choices, Business Week, New York, Jan 12
20. IT Governance Institute. (2001). Board Briefing on IT Governance. Available from: http://www.ITgovernance.org
21. Jamieson R. and Handzic M. (2003) A Framework for Security, Control, and Assurance of Knowledge Management Systems. Handbook on Knowledge Management: Knowledge Matters, Springer-Verlag, New York: 477-505.
22. Kulp, S., Lee, H., Ofek, E., (2004) Manufacturer benefits from information integration with retail customers. Management Science, 50, 4, 431-444
23. Levi, D. S. (2003) Managing the supply chain: McGraw-Hill Professional, USA.
24. Levy, M., Leobbecke C., Powell, P. (2003) SMEs, co-opetition and Knowledge Sharing: The Role of Information Systems, European Journal of Information Systems, 12, 3–17
25. Lin, C., Wu, J.-Y., Hung, H.-C., Lin, B.A (2002) Knowledge management architecture in collaborative supply chain, Journal of Computer Information Systems, 42, 5, 83-94.
26. Marshall, R. S., Nguyen, T., Bryant, S. E. (2005) A Dynamic Model for Trust Development and Knowledge Sharing in Strategic Alliances. Journal of General Management, 31, 1, 41-57.
27. Medcof, J.W. (1997) Why too many alliances end in divorce, Long Range Planning, 30,5, 718-32.
28. Mentzas, G., Apostolou, D., Kafentzis, K., Georgolios, P (2006) Inter-organizational networks for knowledge sharing and trading. Information Technology Management,7, 4, 259-276.
29. Panteli N. and Sockalingam S. (2005) Trust and conflict within virtual inter-organizational alliances: a framework for facilitating knowledge sharing. Decision Support Systems, 39,4, 599-617
30. Pardo A. T., Cresswell A., Thompson F., Zhang J. (2007) Knowledge sharing in cross-boundary information system development in the public sector, Information Technology Management, 7, 293-313
31. Parker, H. (2000) Interfirm collaboration and the new product development process. Industrial Management and Data Systems, 100,6.
32. Rees, J., Bandyopadhyay, S., Spafford, E. (2003) PFIRES: A policy framework for information security, Communications of the ACM, 46,7, 101-106
33. Shafer, G. (1976). A Mathematical Theory of Evidence. Princeton University Press.
34. Shang, H., Anumba, C., Bouchlaghem, D., Miles, J., Cen, M., Taylor, M. (2005) An Intelligent Risk Assessment System for Distributed Construction Teams. Engineering, Construction, and Architectural Management, 12,4, 391-409.
35. Stoneburner, G., Goguen, A., Feringa, A., (2001) Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology.
36. Sun, L., Rajendra, S., Theodore, M. (2006) An Information Systems Security Risk Assessment Model under the Dempster-Shafer Theory of Belief Functions. Journal of Management Information Systems, 22, 4, 109-142
37. Zhang, C. and Li, S., (2006) Secure Information Sharing in Internet-Based Supply Chain Management Systems. Journal of Computer Information Systems, 46, 4, 18-24
38. Zhen, J. (2005) The War on Leaked Intellectual Property, ComputerWorld, January, 5. URL: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=98724
39. Zsidisin, G., Ellram, L., Carter, J., Cavinato, J. (2004) An Analysis of Risk Assessment Techniques, International Journal of Physical Distribution and Logistics Management. 34,5, 397-413