Managing Risk beyond the Control of IS Managers: The Role of Business Management

Susan A. Sherer
Lehigh University
sas6@lehigh.edu

Abstract

While most research has focused on managing technical and project risks in information systems, there are many other components of information systems risk that are currently not evaluated and managed effectively. We identify different sources of risk in both intra- and inter-organizational information systems. Many risks are not well managed because they are beyond the control of the software project manager. We suggest that senior business managers should be responsible for managing organizational risk particularly in the early and later stages of an information systems implementation project. These managers must communicate the importance of new systems and change incentive structures to promote effective system use. We suggest the need to evaluate collaborative risk in inter-organizational information systems and provide guidelines for managing this risk using a joint business management team or a trusted intermediary.

1. Introduction

November 1999: Failed ERP gamble haunts Hershey...A $112 million ERP project blew up in the face of Hershey Foods Corp., causing order processing problems that hampered its abilities to ship candy and other products to retailers. [1]

April 2000: CPFR: buzzword or reality? ...Talking about CPFR and actually making use of it are two different things. [2]

October 2001: Lack of IT integration hurts chem/bio warfare defense...Lack of interoperability among inventory management systems has made it impossible for the Department of Defense to guarantee the availability and effectiveness of its stock of chemical and biological warfare protective suits [3]

January 2002: Now in Bankruptcy, Kmart struggled with supply chain.... Some software projects, intended to help, got scrubbed. [4]

This represents only a few examples of headlines in the last few years relating to problems with information systems investments. It has been estimated that three-fourths of all large systems are “operational failures” because they either do not function as specified or they are simply not used [5]. And almost 1/3 of all software projects are cancelled before the development cycle is complete [6]. While these projects promised potential benefits, their risks were inadequately addressed.

While global expenditure on information systems is increasing, the risk of failure remains. Returns from information systems investments are often less than anticipated because not all risks are successfully identified and managed. The evaluation of information systems projects must incorporate a risk assessment that enables successful risk management. There are different sources of risk associated with information systems investments. Evaluating the risk profile of a project can help companies develop appropriate risk management strategies. A good information systems evaluation process will identify the different sources of risk, develop appropriate strategies to manage these risks, and assign responsibility for risk management to the appropriate managers in the organization.

We suggest that there may be a responsibility gap in many organizations. Senior managers, not just IS managers, must play a very strong role in IS risk management, particularly managing organizational and political risks. Increasingly today companies are sharing information systems, creating new collaborative risks that must be effectively managed. Since inter-organizational relationships are fairly new, not much work has addressed how to manage risks when information systems are shared between organizations.

While the topic of software risk management has been researched for more than two decades now [7], problems with information systems continue to plague organizations. A review of the literature on software risk management...
indicates that most research has focused on either technical or project risk [7-14]. While studies have identified the importance of organizational issues, evidence suggests that this message has not been recognized within the IT community [11]. Not all risks are within the control of the technical or software project manager. Some information systems risks exist because of organizational and political problems within the business units or changes in the organization’s environment. Since these are beyond the control of the software project manager, they are often not included in studies of software risk management. We must understand that there are several different levels of information systems risk management responsibilities in an organization. In addition to technical and project risk management, senior business management must manage organizational change to effectively use information and monitor environmental risk.

Most software risk studies consider risks associated with intra-organizational information systems. Risk management of inter-organizational information systems has received little attention. The Internet has provided an infrastructure contributing to tremendous growth in inter-organizational information systems. Business value now comes from linking disparate organizations’ information systems into extended supply chains. Integrating these extended value chains introduces new risks. Inter-organizational risks can result from inability of organizations to collaborate effectively [2, 15, 16]. Similar to intra-organizational information systems risk, this risk is often beyond the control of software project management. In fact, this risk may require new structures for risk management responsibility. We extend our understanding of intra-organizational risks to inter-organizational information systems by analyzing the source of risk and the level of control of the appropriate risk management team.

In Section 2 we present a risk framework for understanding the source of different components of risk in intra-organizational information systems. We draw from prior research on this topic, providing examples of each risk component, and ways to manage the risk. We use risk categories for intra-organizational information systems derived from previous literature [17, 18]. These components encompass all risks associated with intra-organizational information systems. We then extend this framework to inter-organizational information systems risk in Section 3. Section 4 discusses the implications for risk management today.

2. Intra-organizational information systems risks

It has been recognized that there are many components of risk in information systems use [17, 18]. Understanding differences enables more effective risk management. We believe that improved understanding of the prime source of each risk component will enable more effective assignment of risk management responsibility and authority.

An information system is but one component of an organization that operates in a larger environment. It is part of the work system [19]. The key source of failure may lie within the system itself, but often the source of risk is the organization and/or its environment. Sometimes the source of the risk is the interaction between these factors, for example the system and its organization or the organization and its environment. Table 1 shows three potential sources of information systems risk – the information system itself, the organization, and the environment.

### Table 1. Intra-organizational IS risk

<table>
<thead>
<tr>
<th>Type of Risk</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>Information System (IS)</td>
</tr>
<tr>
<td>Project</td>
<td>IS within the organization</td>
</tr>
<tr>
<td>Organizational/Political</td>
<td>Organization</td>
</tr>
<tr>
<td>Financial</td>
<td>IS/Organization within its environment</td>
</tr>
<tr>
<td>Systemic/Disaster</td>
<td>Environment</td>
</tr>
</tbody>
</table>

Technical risk has the information system as its source. Project risk occurs when attempting to build a system within an organization, thus it lies at the intersection between the information system and the organization. The organization’s political nature, culture, and organizational structure can affect system use, leading to organizational and political risk. Financial risk lies in the interaction with the organization and its environment. The primary source of systemic and disaster risk is the environment in which the organization operates.
2.1 Technical risk: the information system

Technical risk is the risk that the technology doesn’t work, either because the appropriate technology to provide the necessary functionality is unavailable, the wrong technology is used, or the software/hardware fails. Development efforts may attempt to go beyond what is currently technologically feasible [18]. Real time performance shortfalls and straining computer science capabilities can lead to failure [9]. Hardware supporting the software can malfunction. Additionally, since complex software cannot be 100% tested, its reliability cannot be guaranteed [20]. Software errors have had significant consequences, for example, causing failures in military systems [21], telephone networks [22], and medical devices [23].

Technical risks were among the earliest risks that received attention in the literature. In the early 1980s, it was recognized that technology might not support some of the applications that were being built. It was sometimes impossible to achieve required levels of overhead in multiprocessor operating systems, desired computer security protection, necessary speed and accuracy of new algorithms, or desired man-machine performance [24]. McFarlan identified project technology as one of three key risk components [25]. Sometimes the promise of new technology attracts interest before it can fully perform all necessary functions. For example, in the mid 1980s, the New Jersey Department of Motor Vehicles employed a fourth generation language never before used to build a comparable system, resulting in a system crash that left thousands of the state’s motorists driving with invalid registrations or licenses [26].

The complexity of software systems makes it impossible to completely assure its correctness [20]. Technical risk can be reduced by using software engineering process tools [27] and managing development and testing with models that measure software reliability and failure risk [8, 10, 28, 29]. Technical risk can also be managed by utilizing technical experts who understand the technology’s implications. If this expertise is not available internally, the risk can be managed by seeking outside expertise. Project managers play a role in controlling this risk by assigning the correct technical experts (internal or external), and insuring that the proper software development process tools are applied. Thus technical risk responsibility is shared by technical and project managers.

2.2 Project risk: The information system within the organization

Project risk is the risk that the project cannot be completed on schedule or within budget, with adequate performance or in accordance with some measure of project success. Project risk arises when implementing a system within an organization and lies at the interface between the system and the organization. The level of risk is a function of the capabilities of both the organization and the technology.

Information systems project risk management has been a subject of research interest for more than twenty years. Yet project risk continues to plague organizations. In 1982, Brooks reported that more projects went awry for lack of calendar time than all other causes combined [30]. A mid 1980s survey of the clients of major accounting firms revealed that 35% had major overruns [31]. And there has been little change today. In 1999 The Standish Group survey of several thousand software development projects found that only 26% were completed on time and on budget. Twenty eight percent were canceled before completion and 46% were completed over budget and behind schedule, with fewer functions and features than originally specified [32].

Several studies have attempted to identify all the different software project risks [9, 13, 14, 25, 33]. Risk identification is the first step in risk management [7, 34]. Software project risk includes technical and behavioral risk components [34]. Organizational issues are the most dominant project risk factors, but they are satisfactorily treated in less than a third of systems development projects [11].

Project risk management encompasses formal planning, internal integration, and user participation [7]. Standard project management tools focus primarily on planning and internal integration. Participative design methods help encourage user participation [35].

Successful project managers focus primarily on risks over which they have limited control or influence, e.g. lack of adequate user involvement or frozen requirements. They focus to a lesser degree on risks over which they have complete control, such as misunderstanding the requirements and lack of effective project management [14]. However, successful project managers rank low those factors over which they...
have no control or influence. These risks include conflict between user departments, change in ownership or senior management, staffing volatility, number of organizational units involved, multi-vendor projects, and new subject matter [14]. This is not surprising because these are not the primary responsibility of the project manager. However, these are significant risk factors in organizations today. Creating a climate for change has been recognized as a significant risk factor in enterprise system implementations [36]. The highest risk that is most difficult to manage is changing organizational culture [37]. The project manager’s responsibility is limited to project culture. Project culture is affected by organizational culture but the primary responsibility for organizational culture is senior business management. Not recognizing these risks as distinct from information systems project risk may not only underestimate their significance to organizations today, but may result in less effective risk management.

2.3 Organizational/political risk: the organization

Organizational/political risk is the risk that the system is not effectively used because of organizational structure and internal politics. This risk include the risk factors that successful project managers identified as “risks outside purview of project manager”, including conflict between user departments, change in ownership or senior management, staffing volatility, number of organizational units involved, multi-vendor projects, and new subject matter [14]. It includes client based “people problems” such as unrealistic user expectations, lack of real user customer of the project, disagreement amongst customers’ people on project goals, personal deficiencies on the part of the customer’s project manager; user resistance, and the presence of hidden agendas or “nasty” politics by the customer [38].

One example of organizational/political risk is detailed in [39]. An expense tracking system implemented at the Tiger Creek paper mill provided the opportunity to lower mill operations costs. Operators found that the information from the system empowered them to better manage the mill. However, managers threatened by the new found power of the operators adopted procedures to use the system to impose rules on the operators and check up on them, minimizing the operators’ ability to optimize the process. The cost savings from the system reached a plateau; and the full system potential was not realized because of the threat to management’s power.

More recently, one factor contributing to Kmart’s recent bankruptcy was its failure to build a supply chain planning and execution system to effectively manage demand. This was attributed to executive management’s historic inability to fully execute on innovative IT efforts [4]. While Kmart contracted with i2 Technologies for TradeMatrix, they never implemented the system. They decided to reengineer their business first and never got beyond that.

Because the risk factors in organizational/political risk are outside the control of the project manager, we believe that project managers do not perceive them as major risks and do not develop strategies to minimize their impact. However, these risks are very evident in organizations today and may account for the fact that organizational issues are only successfully treated in between 10 and 30% of all projects [11].

Organizations that clearly identify and understand this risk may be better able to manage it by assigning responsibility to senior business managers. The risk management techniques involved here are similar to some of the behavioral based strategies used to manage project risk. In particular, they involve change management techniques to insure that the organization effectively implements and uses the system. This requires external change agents, top management support, change communication initiatives, and changed performance metrics. While project managers can devise strategies to cope with some of these issues [38], the distinction between the strategies for managing behavioral project risk and organizational/political risk is that the prime responsibility for risk management lies with external constituents, not the project management team. Moreover, this is one risk that is often not more effectively managed with outsourcing. While consultants can be helpful in determining what has to change, this is a risk management tool that most often should be managed from within.

2.4 Financial risk: system/organization in its environment

Financial risk is the risk that the system does not achieve expected financial benefits [17]. Financial risk may occur because development costs are too high, as a result of ineffective
project risk management. High costs also result from ineffective organizational/political risk management that leads to poor system use. For example, users may not be provided with requisite skills. Zuboff illustrated that computer use requires intellective skills that are very different from action centered skills [39]. Finally, all benefits may not be achieved because the environment changes. For example, a company implementing a new ERP merges with another firm using a different ERP system that is subsequently chosen as the company standard. Financial risk is interrelated with all the other risks. Managing this risk is primarily the domain of executive management who must insure that the appropriate systems are selected so that benefits can be achieved. However, IS project managers play a role in managing development costs, which affect financial risk.

2.5 The environment: systemic and disaster risk

Two risks whose source is primarily the business’ external environment are systemic and disaster risk. Systemic risk occurs when a system is so successful that competitive response reduces the value of the system or unfavorable regulatory changes are made in response to the project’s success [17]. For example, the developers of the SABRE and APOLLO computerized reservation systems were forced to eliminate screen bias when they became major channels for airline reservations. Traditionally, there have been few methods to manage this risk. Strategic planning and scenario analysis can help anticipate this risk and provide time to develop appropriate responses [40]. Managing this risk is the responsibility of executive management who has the strategic perspective of the firm in mind.

Disaster risk is the risk that the system is harmed by external disasters such as flood, fire, or other natural disasters, terrorism or war. Nineteen percent of CIOs recognize the importance of disaster recovery plans; 75% of them have such a plan [41]. Risk management techniques include back-up sites, data recovery plans, and insurance policies. Disaster risk is receiving additional scrutiny as a result of September 11. Committees such as the Society of Information Management’s IT Civil Defense workforce have formed to improve disaster risk assessment and management. Managing this risk is a shared responsibility of technical and business management.

3. Inter-organizational information systems risks

Business success today often depends upon integration of systems shared between value chain partners. As inter-organizational information systems (IOS) are becoming increasingly important, the risks associated with these systems must be understood and managed. While they have many of the same risks as intra-organizational information systems, there are some new risks associated with these systems as they interface with different organizations and their environments. Table 2 extends our risk framework to systems shared by more than one organization. One new set of risks is associated with the integration of disparate systems. While companies have struggled internally with incompatibility risk, integration problems are exacerbated when more than one company directly shares information as there is a greater chance that incompatibilities exist and the responsibility for reconciling differences is shared by managers in different organizations. As systems become more accessible to external users, security risks increase. Inter-organizational information systems also involve collaborative risk, the risk that partners do not effectively share and use each other’s information. Finally as systems are available to customers and suppliers in an open arrangement, there is the increased opportunity for external parties to gather information that could be used competitively against a company.

Table 2. Inter-organizational information systems risk

<table>
<thead>
<tr>
<th>Type of Risk</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incompatibility</td>
<td>Inter-organizational systems (IOS)</td>
</tr>
<tr>
<td>Security</td>
<td>IOS within the organizations</td>
</tr>
<tr>
<td>Collaborative</td>
<td>The organizations</td>
</tr>
<tr>
<td>Competitive</td>
<td>IOS/organizations within their environment</td>
</tr>
</tbody>
</table>

3.1 Incompatibility risk

Incompatibility risk is the risk that multiple systems cannot effectively share data because of incompatible technologies. Connections or interfaces between information systems may be
improperly designed, or designed connections may have atrophied [42]. For example, intersystem links among patient, care team, and pharmacy databases are often overlooked in large hospitals and medical systems, leading to unacceptably high numbers of errors [42].

While incompatibility risk exists integrating systems within a single organization, it has been managed through the acquisition of compatible technologies and/or the use of middleware and enterprise application integration software. When integrating systems between organizations, costly proprietary technologies have kept smaller firms, in particular, from electronically linking with others through traditional EDI [43, 44]. Today, however, incompatibility risk is decreasing. It is increasingly managed with non-proprietary technologies such as XML and Internet based EDI. Web services provide an opportunity to further decrease this risk.

3.2 Security risk

Security risk is the risk of unauthorized access to systems that can result in alteration or theft of information. Just one computer hacker in 1995 stole information worth more than $1 million, including thousands of credit card numbers from numerous businesses [41]. This risk is managed through technical measures, policies, procedures, and controls. While security risk exists for intra-organizational information systems, this risk is compounded with IOS where there is less access control. Technical risk management methods such as authentication, encryption, firewalls, and VPNs have improved. However, control procedures can be more difficult to monitor. Risk management is compounded by the fact that people external to the organization accessing the system are outside the control of the organization.

Today security risk is receiving increased attention. It is estimated that corporations will boost information technology security spending by 18% in 2002 and the federal government will more than triple its IT security budget from $1.3 billion to over $4.1 billion by 2006.

Ultimately, the problem lies beyond any technology solution [45]. While selecting and implementing security measures is the domain of the IS project manager, security at the organizational culture level is senior management’s responsibility. Managing security risk involves defining and enforcing guidelines for data handling and access privileges [19]. In some organizations, a cultural change is required. Changing the culture among users of information is often beyond the control of the software project manager. Senior business managers must focus on development of incentives to promote enforcement of security policies and procedures.

3.3 Collaborative risk

Collaborative risk is the risk that the information needed to collaborate is not shared effectively between business partners. While the system itself may provide all the functionality to improve collaboration, collaborative benefits will not accrue unless the participants are willing to share information and use the systems effectively. A 1993 field study in the consumer-packaged goods industry suggested that the economic benefits from improved coordination through IT might not be realized fully in practice. Checkout scanner systems and information systems permitted more tightly coupled logistics operations in the distribution channel. However, there was considerable resistance by retailers because they felt that their bargaining power would be eroded, precluding their sharing in the economic benefits [46].

Interdependencies, power of the EDI initiator, and trust toward partners have been critical issues in EDI adoption [44]. Due to the network nature of EDI, the benefits to an EDI user are a function of the investments of its trading partners [43, 47]. As more trading partners became EDI-capable, a firm received higher benefits due to its increased ability to collaborate with more partners. Therefore, inter-organizational pressures played a critical role in lowering collaborative risk, making it possible to effectively share data with more partners.

Today Collaborative Forecasting and Replenishment (CPFR) systems allow retailers and manufacturers to compare demand and supply forecasts in order to synchronize their value chains. Getting business to make such information available is no small task [48]. A key challenge is getting upper management to buy into the idea of handing out sensitive corporate data to suppliers, data that could reach competitors if it were passed along [2]. CPFR requires participants to share information regarding events such as promotions and store openings that might impact forecasts. Often they are uncomfortable sharing promotional information [2]. They require participants to communicate and resolve variances within item
level forecasts. While CPFR systems provide information about deviations between forecasts, they do not self adjust plans. Participants must take actions to revise their forecasts and change their patterns. Collaboration is still in the early evangelical stages [16]. Customer and supplier companies must communicate more and share previously unshared information [16]. The systems can only support collaboration; much more cultural change is required. “The goal of CPFR is to eradicate the buyer/seller viewpoint….implementing CPFR successfully involves a frontal lobotomy. Most business processes have to be rewritten,” according to Andrew White of Gartner [49].

Collaborative risk management can be accomplished if business partners change their cultures. Specific change management techniques are required. Sara Lee Casual Wear, during their three-month pilot study with Wal-Mart found that they had to learn to learn to collaborate to make CPFR work, involving tremendous effort [2]. Smaller companies who find it very difficult to collaborate may choose to use an intermediary to manage collaborative risk. A neutral external party can facilitate the interaction. For example, when a group of small independent firms joined a manufacturing network, they found that successful cooperation occurred only after they formed a separate organization, Agile Web, Inc. They used the president of the company as a neutral party who facilitated their collaborative efforts. While it looks like internal collaboration, it was really collaboration from the outside rather than internally [50].

3.4 Competitive risk

Competitive risk is the risk that a company’s ideas, operating procedures, customer records, etc. become publicly available and can then be used against them in a competitive environment. Competitive risk emphasizes the use of proprietary information where a competitor improves performance at another organization’s expense; whereas collaborative risk emphasizes lack of information sharing that could result in improvement for both parties. Lawsuits over trade secrets are common among technology vendors. Eli Lilly and Co. has all its IT workers and contractors sign non-disclosure forms to prevent them from discussing any of the company's business plans and pharmaceutical product development, as well as technology [51]. As companies make information readily available on the internet, there are more opportunities for competitors to learn about other companies' products, services, and strategies. Imitators can steal innovations [52]. Companies must protect their intellectual property in an increasingly difficult environment.

4. Conclusions and implications for risk management

Most of the software risk management literature has focused on the identification and development of risk management tools directly related to the system, the technology, or the project - the interface between the system and the organization. Yet the risks faced by organizations implementing and using information systems today are much more complex and wide ranging. The information systems project manager cannot simply manage these risks. They require much broader authority and management clout. Senior management must recognize their role and responsibility for information systems risk management if improvements are to be made in the poor records of IS implementations to date. This is increasingly important as more companies participate in inter-organizational information systems.

We believe that technical, project and incompatibility risks can be managed effectively today using available risk management tools. If companies lack expertise in these areas, outsourcers can help. Selective outsourcing has been successfully used to mitigate risk [53]. However, internal expertise should still be retained to achieve full management control and visibility [54]. We propose that a major purpose for retaining this expertise is to manage the behavioral components of project risk. Internal personnel help manage behavioral project risks such as user support, experience, and role definition. These risks are managed with behavioral strategies such as generating user and management support and institutionalizing system practices [34]. Outsourcers may have difficulty providing these behavioral risk management strategies. However, with adequate change management tools and project management capabilities, these risks can be effectively managed today.

Systemic, disaster, and competitive risks are difficult to manage. Since they are initiated by activities outside the control of the organization, the most effective strategies are anticipatory and...
environmental monitoring strategies. One alternative is to insure against risks that cannot be controlled. Insurance is one of the oldest strategies for dealing with disaster risk. Standard policies insure against threats such as fire and hardware failure. Even software errors and omissions policies are available [29].

It is the evaluation and management of organizational/political and collaborative risk where we can make significant progress. We believe that companies can decrease their organizational/political risk by recognizing the need to explicitly assign risk management responsibility beyond the IS project manager. The identification of these risks as distinct from information systems project risks draws attention to their unique needs. Researchers have found that successful projects tend to conform to Lewin’s theory of planned change, which suggests three sequential phases of the change process [55]. The first stage, unfreezing, creates a climate for change. The second stage, moving involves analysis, design, and installation. The third stage, refreezing, institutionalizes the change [56]. Stage 2 of Lewin’s theory is the responsibility of the information systems project manager. The IS manager focuses on reducing the risk of failure of analysis, design, and installation. However, stages 1 and 3 are the responsibility of senior management. We suggest that high risk occurs today in the freezing and refreezing processes. Information systems managers cannot unilaterally change and institutionalize new business culture. Thus, they cannot manage the risk associated with these aspects of change. Figure 1 suggests how information systems and senior management’s risk responsibilities can be effectively allocated within the three stages. It also shows some risk management strategies that can be implemented in each stage. We propose that senior managers have specific responsibilities to manage risk, particularly in the first and third stages. IS management’s risk responsibilities are confined to stage 2.

Organizational development (OD), the planned process of developing an organization to be more effective in accomplishing its goals, includes effective change interventions that can be used by senior managers [57, 58]. These focus on developing the structures and systems within the organization, with primary emphasis on human resources, to improve organizational effectiveness. One of the underlying principles of the planned change model is the sharing and communication of information about the change [58]. Open dialogue and training supports the unfreezing process. The information systems project manager cannot affect these changes without significant involvement of senior management. In stage 2, IS managers can use both process and project management strategies to reduce risk in moving the organization to the new system. While IS managers must be supported by senior managers, it is during this stage of the project that the IS project managers can most effectively manage risk. Change management is the process of reducing resistance to the change and increasing support and commitment for it, whether that be a change in process, structure, technology, reward systems, management practice, or culture [57]. Part of the social process of new system implementations involves adoption of new solutions, which requires rigorous organizational change. This change often only occurs if senior management places in place incentives for cultural change. Change management involves effectively balancing forces in favor of a change over forces of resistance [59]. Senior management must insure that change forces are rewarded greater than resistance forces. Thus senior management, not IS management, is primarily responsible for change during the freezing process.

Figure 1. Managing risk for successful projects

Can organizational/political risk management be outsourced? Cultural change is often more easily accomplished through internal change agents. However, there may be situations that are so politically charged, that progress will not be made without external help. Internal IT monopolies promote complacency and create organizational obstacles to continuous improvement [54]. In these cases, senior management can be aided by external expertise. But, similar to the management of project and technical risk, it is imperative that a firm continue to maintain responsibility for risk management. IT applications that cross business
functions may be difficult to outsource because vendors do not understand the implications that IT has for other business processes [54]. This risk is compounded when applications cut across organizational boundaries. “While some activities can be outsourced, many others require management’s attention, protection, and nurturing to ensure current and future business success.” [54]

Collaborative risk management requires new risk management structures. We contend that two possibilities may evolve for collaborative risk management: 1) joint risk team and 2) risk intermediary. The joint risk management team involves representatives from all participants who have managerial responsibility for effecting change within each of their respective organizations. These will be business managers; not information systems managers. If all companies do not participate in the joint risk management team, effective collaboration will not occur. If the organizations cannot commit to direct collaboration, then risk intermediaries may be the only effective solution to manage collaborative risk. The small and medium size companies that came together in one of the first manufacturing networks funded by ARPA, were not able to collaborate with each other to gain new business. Only after they incorporated as Agile Web, Inc. and brought in a president who was their trust intermediary were they able to successfully gain new business [50].

This study has developed a model that suggests a greater role for senior management in risk management, particularly management of organizational/political risk. We have also suggested specific mechanisms for managing inter-organizational risks. This study provides some important guidelines to practitioners for managing organizational/political risk. We have also gathered further evidence of management in both intra and inter-organizational risk management.

Future research will study the role of senior managers in information systems risk management. We will gather further evidence of the contribution of organizational/political risk to overall information systems risk. We will investigate how senior managers can effectively support information systems managers in reducing risk, verifying the usefulness of the model suggested in Figure 1. We will also study some collaborative efforts in inter-organizational information systems and look at the factors that led to their success and lowered their risk.

5. References

[31] Rothfeder, J., "Its late, costly, incompetent, but try firing a computer system", in Business Week, 1988, p. 164-165.
[43] Bouchard, L. "Decision criteria in the adoption of EDI", in ICIS. Orlando, FL, 1993