Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 1997 Proceedings

Americas Conference on Information Systems (AMCIS)

8-15-1997

The Risky Business of Managing Information Systems

Susan A. Sherer
Lehigh University, sas6@lehigh.edu

The Risky Business of Managing Information Systems

Susan A. Sherer
Lehigh University,
621 Taylor Street, Bethlehem, PA 18015,
610-758-3424, SAS6@LEHIGH.EDU

Abstract

IS managers are faced with many different risks such as project, capability, financial, and maintainability risks, caused by a variety of technical, organizational, and environmental factors. We found that senior IS managers in several diverse organizations focus primarily on managing organizational contributors to risk, in particular instituting various change management strategies to manage functionality and systems integration risk. Managers today are concerned about the financial risk resulting from lack of technical procedures to justify IS investments.

Introduction

Information systems (IS) executives manage many risks that could potentially cause economic and even physical loss to their businesses. As organizations become increasingly reliant on their information systems for critical functions and the complexity of these systems increases with new technology, the number of different risks and the degree of risk grow substantially.

There are many different types of risk faced by a senior IS manager [Boehm 88, 89, Clemons 91, Schneidewind 87, Sherer 95]. **Project risk** is the risk that a development project cannot be completed due to *personnel*, *schedule*, or *process* problems: personnel lack capability to execute a project, project cannot be completed on time or within budget, or the organization does not have an effective development process. Once a system is developed, the IS manager is faced with **capability risk**, risk that the system does not provide necessary *functionality* or *reliability*, meet *performance* needs, or *integrate* with other systems and processes. **Financial risk** is the inability to achieve an adequate return on investment. External threats to *security* and property are also a concern. Finally, systems may suffer from **maintainability risk**, lacking the capabilities to be fixed or adapted to new environments or technology.

Each of these different risks may be caused by the following factors [Sherer 95a]: **Technical:** procedures, technical knowledge, conceptual models, hardware, and tools are unavailable or inadequate to accomplish necessary tasks; **Intra-organizational:** formal and informal arrangement of human resources impede performance of necessary tasks due to the nature of the social organization, belief and meaning systems, power relationships, norms of conduct, and lines of communication; **Inter-organizational:** relationships with external suppliers, developers, or strategic partners are not well managed; and **Environmental:** competitive, regulatory, market, or technology change alters the viability of the infrastructure and applications.

Using this causal framework, we reviewed existing literature to understand the tools and techniques that have evolved for managing risk [Sherer 95a]. This provided an understanding of those causes of risk that currently can be effectively managed as well as those that are still problematic for IS managers. We found that technical risk management tools have been most widely developed and implemented. While there are a number of risk management techniques for managing intra-organizational causes of risk, we expect that senior IS managers still focus most of their efforts on the management of these contributors to risk. We also hypothesize that IS managers will need to increasingly address inter-organizational risk as businesses form more of these relationships [Sherer 95b]. Environmental risk is difficult to manage except through continual planning, flexibility, and re-evaluation. This study reports on the results of a preliminary exploration of these hypotheses through a study of the risks currently faced by some senior IS managers in three different organizations.

Research Methodology

We used the case study method in this exploratory phase of our research. Our objective was to use the causal framework from [Sherer 95] to help identify major risks currently faced by some IS managers, strategies used to cope with these risks, and factors that may cause the most significant risks. We specifically chose different size organizations in very different environments and industries in order to initially see if our hypothesis had broad support. The three different organizations are briefly described in Table 1.

We used a structured interview protocol based upon our theoretical causal model, along with observations and archival sources. Interviews with a senior IS manager in each organization were structured by our causal

Table 1. Description of Organizations

	Type of Organization	Size/Scope of Organization	Number of IS Personnel	Key IS Management Responsibilities
MANU	Manufacturer - industrial gases and chemicals	Fortune 1000	450	Establish computer architecture; Manage standards; Desktop computing; LAN administration; Engineering support; Database administration
HEALTH	Regional hospital	800 bed	70	Operations; Network support; Systems analysis; Customer service
ACAD	Private university	6000 students	150	Information and technology support for academic programs and campus life. Includes: computing, telecommunications, library

framework. By focusing on each of the causes of risk to elicit risk identification, we hoped to widen IS managers' assessments of risk from those that were at first most "available" and "representative" for recall [Slovic et al. 80, Tversky & Kahneman 74]. In each case we examined the technical skills, organizational structure, inter-organizational relationships, and environmental factors that might affect the risk profile.

Table 2 summaries the major risks and management strategies identified in each environment along with our classification of the type of risk and its cause.

Causes of Risk

We found that IS managers stressed the significance of risks caused by organizational factors, particularly risks resulting from individuals who will not change. In the manufacturing company, the inability of individuals to accept change could impede progress towards standardization and the global seamless architecture required for more effective competition. Individual workgroups, accustomed to developing unique nonstandard systems, were not easily convinced to accept change. In the hospital, the inability of physicians to adapt to new technology could mean needless expenditures of funds in a cost conscious industry. Physicians have traditionally operated as independent entrepreneurs; they do not like to be told what to do and their environment has traditionally enabled them to control their own destiny. Thus there is a high risk that they may initially endorse change but opt not to use new technology once it is in place. In the academic environment, the inability of participants to adjust to the recent merger of the library and computing center could inhibit joint efforts to improve the information resources infrastructure. Change management techniques, focusing on communications, education, and restructuring, were the most prevalent risk management techniques in use by senior IS managers.

Technical risk factors did not contribute to any of the major risks in these organizations except financial risk. The IS managers had all instituted many technical risk management tools to reduce project, capability, and maintainability risks. However, lack of tools and techniques to justify IS investment to senior management [Keen 91] were continuing concerns for all three organizations. Each feared that senior management will not continue investing in IS unless assured of justifiable returns. All were frustrated by lack of methods for justifying their investments particularly in infrastructure. In the hospital, cost reduction efforts put continual strain on the IS department as they were called upon to help reduce costs in other departments while continually reducing their own costs.

Inter-organizational risk was of most concern to the university because of its strong dependence on outside vendors. The manufacturer and the hospital were not as dependent on outside vendors, striving for self sufficiency in order to minimize inter-organizational risk. However, it is expected that these organizations may be atypical and that more organizations will work with vendors and enter strategic partnerships, requiring IS managers to effectively manage this contributor to risk.

Environmental factors were most prominent in the health care industry where the environment is changing most rapidly. Managers were concerned that the IS organization's performance could be hindered by personal and organizational fear that new systems would never be used, supplanted by systems of acquiring organizations. Since IS managers cannot control the environment, they try to remain both flexible and adaptable with their choice of technology and personnel.

Table 2. Major Risks

	Major Risk	**Risk Management Strategies**	**Type of Risk**	**Causal Factor**
MANU	Inability to integrate systems into global seamless architecture	Education; Create desire for standardization; Share stories and analogies; Collaborative efforts	Integration Capability	Organizational
MANU	Justifying further investment	Provide feedback to senior management; Produce quality products	Financial	Technical
HEALTH	Users (physicians) will not use technology once its implemented.	Marketing and education; Shadow users to assess needs; User/IS committees	Functionality Capability	Organizational
HEALTH	Remaining technologically current in an environment of cost reductions	Project management	Financial	Technical
HEALTH	Acquisition and merger fear	Modular, flexible, adaptable systems; Morale building through honesty, open communications, personal relationships	Capability	Environmental
ACAD	Inability of individuals in traditionally distinct departments to work together effectively.	Teams; New terminology to induce "out of the box" thinking; Functional reorganization	Integration Capability	Organizational
ACAD	Mistiming of major investments	Rechecking new technology against current investment	Financial	Technical
ACAD	Outside vendors not providing necessary support	Long term strategic planning; Vendor management	Capability, Mainainability	Inter-organizational

ACAD	Overselling technology	Communication; Reorganization	Functionality Capability	Organizational

Conclusions

A causal framework was used to understand the key risks in IS organizations in several different industries. Our exploratory study indicated that organizational factors are key contributors to all risks. Change management tools are among the most common risk management tools. Tools to manage financial risk are needed by IS managers. Inter-organizational risk is a concern for managers involved in collaborative efforts. Environmental factors contribute to risk most prominently in industries experiencing rapid change.

Future research will involve indepth case studies in a much broader sample of organizations. We will focus on the risk management tools in use by a number of different IS managers in a larger number of firms in different industries. The study will focus primarily on tools for managing organizational and financial risk. We will attempt to relate specific risk management tools to the risks that they address. In addition, we will focus on the outcomes, relating risk and risk management tools to various performance measures. Our objective is to develop a rich set of guidelines for understanding and managing risk.

Additional research on interorganizational risk is currently in progress. We are focusing on a specific type of interorganizational relationship to understand strategies used to manage interoganizational risk. Our current study of networks of small manufacturers is helping us understand the risks that arise from these relationships and the risk management tools used to address these risks [Sherer 95b].

References

Boehm, B. (ed), Software Risk Management, Washington: IEEE Computer Society Press, 1989.

Boehm, B., "A Spiral Model of Software Development and Enhancement," Computer, May 1988, pp. 61-72.

Clemons, E., K., "Evaluation of Strategic Investments in Information Technology," CACM 34(1), 1991, 22-36.

Keen, P. Shaping the Future: Business Design through Information Technology, Mass.: HBS Press, 1991.

Sherer, S.A. "The Three Dimensions of Software Risk," Proceedings HICSS 1995a, 369-378.

Sherer, S.A., "Risk in Interorganizational Information Systems," Proceedings AIS, 1995b, 14-16.

Slovic, P., Fischoff, B., Lichtenstein, S., "Facts versus Fears: Understanding Perceived Risk," Societal Risk Assessment: How Safe is Safe Enough?, ed: Schwing, Albers, NY: Plenum Press, 1980.

Tversky, A., Kahneman, A., "Judgment under Uncertainty: Heuristics and Biases," Science 185, 1974, 1124-1131.