

**Including Technical and Security Risks in the Development of Information Systems: A
Programmatic Risk Management Model**

Security is increasingly becoming a critical focus in information systems projects. With more networks, mobility, and telecommuting, there is an increased need for an assessment of the technical and security risks. These risks if realized can have devastating impacts: interruptions of service, data theft or corruption, embezzlement and fraud, and compromised customer privacy. The software risk assessment literature (for example, Schmidt et al., 2001, Barki et al., 2001, and Lyytinen et al., 1998) has focused primarily on managerial or development risks. With the increasing focus on technical and security risks, theoretical risk models need to be developed that can provide a framework for assessing and managing the critical technical and security risk factors in conjunction with the managerial and development risks. This research seeks to model this problem by extending risk models originally developed for large-scale engineering systems.

Submission for Research-In-Progress Track

Submission Word Count:

Research Objectives and Questions

As technology improves and networks become increasingly intertwined, security needs to be a critical focus when developing information systems. Today's information systems projects are grasping with how to make the system open for the right users to access and share data but closed enough to keep the wrong users out. Technical risks must now include threats to the system (such as functionality and reliability) and threats to the data (such as integrity, confidentiality, and availability) (Denning, 1999). Also, in the current economic environment, the resources available for systems development are tightly constrained, thus requiring trade-offs between more risky, cutting-edge systems and more robust systems with modest functionality.

Depending on the application, the damage from technical and security problems can range from inconvenient to expensive to the loss of irreplaceable data or public trust. For example, in December 2001, because of the lack of security in the information systems for the Bureau of Indians Affairs (BIA), the U.S. Department of the Interior disconnected the BIA and seven other departmental bureaus from the Internet. Fontana (2002) states, "Six months earlier, then-BIA CIO Dom Nessi publicly admitted that his department had no real security, no firewalls and potentially could be hacked by a high school student." Further, Fontana (2002) goes on to state, "Observers also are scratching their heads over how DOI, which has received \$2.3 billion in IT budget money since 1999 and has an IT staff of 2,272, could not muster the resources to correct no-brainer security holes at BIA, such as lack of firewalls or blank administrative passwords." Most DOI bureaus were disconnected from the Internet for three to four months, many people were inconvenienced (e.g., campers could not reserve tent sites in any national park and individuals could not apply for summer jobs at the parks), and the financial implications were enormous. In general, costs of systems failure must include: 1) costs of

reproducing lost information, 2) repercussions to the organization of not readily available system access or information, 3) cost to organization if information was released, altered, or destroyed, and 4) loss of public confidence (Denning, 1999).

For almost four decades, research in information systems development and software risk assessment has cited statistics such as 46% of the development projects surveyed were completed over budget and past original deadlines and 28% were cancelled before completion (Standish Group, 1998). In an attempt to remediate the continuing problem of information system failures, software engineering and information system researches developed rigorous systems analysis and design methods (for example, Whitten and Bentley, 1998) and conducted numerous surveys in an attempt to systematically organize critical risk factors (Schmidt et al., 2001, and Barki et al., 2001). These approaches provide valuable input to a risk management program to the degree that they help identify potentially difficult projects that require special attention or additional resources (McFarlan, 1982). Such an approach is based, however, on past experience and assumes that there are sufficient similarities between the IS systems that have been studied and the considered new ones. For example, in the survey of risk factors compiled by Schmidt et al. (2001), not a single one of the risk factors had to do with any technical aspects of the system, and Jiang and Klein's (2000) study of software development risks also does not include system technical performance. While the performance and capabilities of both hardware and software have improved significantly over time, with more networks, mobility, and telecommuting, we need to assess and mitigate technical and security risk factors in conjunction with management risk factors in the development phase.

The framework described here is based on probabilistic risk analysis and decision analysis and supports project manager's resource allocation decisions during systems

development. Managers can allocate resources to: technical system improvements (higher reliability and security), functional enhancements (more data access and better features), and budget reserves (funds to solve development problems that arise). Resources allocated in each area affect either the probabilities or the values of the possible project outcomes. The objective of this research is to demonstrate, for the development of an information system, how a project management framework based on a probabilistic model of the system's performance, the risk factors, the risk mitigation options, and the design alternatives, can maximize the expected project outcome through the optimal allocation of project resources. The model uses a utility function to explicitly examine the tradeoffs between minimization of the probability of a project's failure and maximization of the expected benefits from its performance.

The primary result of the research is a theoretical framework to guide design and resource allocation decisions to minimize the risks of information systems failures. This framework can be modeled using Excel and off-the-shelf decision and risk software to create a prototype decision support system to provide quantitative analysis of risk tradeoffs and resource allocations for information systems development projects.

Theoretical Foundations of the Study

The framework is based on probabilistic risk analysis (PRA) and decision analysis (DA) where PRA is used to quantify the risk of potential alternatives and DA provides the framework for including values and preferences to determine if the potential benefits are worth the associated risks. PRA was developed originally in electrical engineering, aeronautics and astronautics, and the nuclear power industry [see for example, Henley and Kumamoto (1992), Garrick (1984), Kaplan and Garrick (1981), and Fragola et al. (1994)] to compute the probability

of failure of complex systems. The PRA model links the reliability of individual components and the overall system configuration to quantify the overall technical failure risk. This approach to risk assessment is similar to that advocated by Boehm (1991) but requires the quantitative assessment of probabilities and outcomes. A probabilistic risk analysis (PRA) of the system is required to determine how and where money should be spent. The probability of a technical failure given investments in reinforcement can then be expressed as a function of the probabilities of the different failure modes based on the design configuration, the investments in the reinforcement of the components, and the effects of these investments on the component reliability.

The primary objective of decision analysis is to determine which alternative course of action will maximize the expected utility for the decision maker. It is based on the existence of a set of logical axioms and a systematic procedure to aggregate probabilities and preferences based upon those axioms (Bodily, 1992). Unique to decision analysis is the creation of a preference model to evaluate the alternatives and possible consequences. This preference model includes information about value tradeoffs, equity concerns and risk attitudes (Keeney, 1982).

The need for this decision-risk framework is justified by Barki et al. (2001), McFarlan (1981), and others [for example, Jiang et al. (2001), Ropponen and Lyytinen (1997), and Nidumolu (1996)]. Their research shows that for complex information system development problems, project management tools that help identify and mitigate risks are key factors in determining project success. Also, Keil et al. (1998) document the need to establish the relative importance of the risks so managerial attention can be focused on the areas that constitute the greatest threats, but their study included little discussion of technical risks.

While contingency theory approaches rather than risk management approaches are predominant in the IS implementation literature [for example, Cule, et al. (2000), Ropponen and Lyytinen (2000), and Nidumolu (1996)], key structural components of the decision-risk framework as described further are derived from software risk management literature [for example, Barki et al. (2001) and Nidumolu (1995)] and also information security research [Denning (1999) and Greenstein and Feinman (2000)].

Model Framework

As shown in Figure 1, managers must carefully balance information assurance and operational capability. For example, the more capabilities that you provide your employees to remotely access and alter files that they store on the network, the more security is required to prevent unauthorized users from accessing and altering network files.

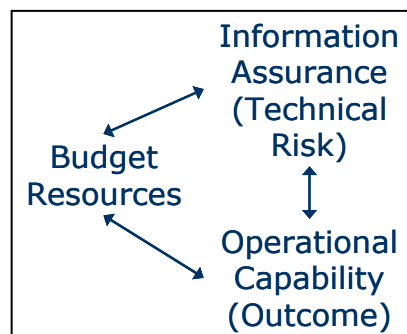


Figure 1 – Factor Trade-offs

And this balance must occur within the available budget resources and with consideration for all the traditional management risks identified by the software development risk literature [for example, Barki et al. (1993), Schmidt et al. (2001), and Boehm (1991)] such as lack of top management commitment, misunderstanding the requirements, failure to gain user commitment, changing scope and objectives, etc.. This distinction between management risk factors and technical risk factors is consistent with the distinction made between process and product

performance in the literature [Nidumolu (1995), and Barki et al. (2001)]. The optimal balance can be determined based on maximizing the expected utility for the design alternatives. The utility of the outcome is based on both the total costs spent (Z) and the operational capability of the final system (D) given that the system works. The system working is defined by a PRA model of the system that quantifies the probability of technical failure ($p(\text{TF})$). Budget resources can be spent to enhance the operational capability of the system (E) and can be spent to reinforce the technical reliability (I). Both categories of additional budget must be included in the total costs spent (Z) and the more that is spent, the greater the likelihood for cost overruns. For significant cost overruns, the utility of Z is zero ($U(Z) = 0$). The expected utility of an alternative (A) is thus:

$$EU(A) = U(Z, D_A | E) \times (1 - p(\text{TF} | I)) \quad (1)$$

The decision maker thus faces two types of uncertainty: 1) the possibility of development problems, e.g., specific functions may not be completed on time, which contributes to the total cost of the system (Z) and 2) the system's performance in operations (i.e., $p(\text{TF})$). The optimal design and the level of reserves are then chosen to maximize the decision maker's overall utility function for the system based on these factors. This framework was originally developed based on case studies of NASA's unmanned space projects (Dillon et al., *in press*) and has been modified here to include information technology specific-risks and factors.

Consider briefly a web server example. Functions include verifying accounts, storing files, serving requested data, tracking users and creating logs, providing maintenance and administrative capabilities, and ensuring security. Example failures include the system is not available and/or the user cannot access it, data confidentiality is lost, or the integrity of the server is lost either from proper data being corrupted or from improper data or files being added. These

failures can result from several initiating events as shown in Figure 2 including attempted attacks, system administrator errors, hardware or software failures, or some transient events (e.g., cut cables or power outages). Cost consequences may include losses from fraud, lost revenues from lower sales or fewer users, costs from lost time in terms of productivity, and/or the intrinsic value of the lost data. Example development alternatives include firewalls (various hardware and software alternatives), different software operating system alternatives, various hardware configurations of multiple servers, cryptography/encryption, and improved development and maintenance processes including more code reviews, better configuration management, more training, and automated software updating.

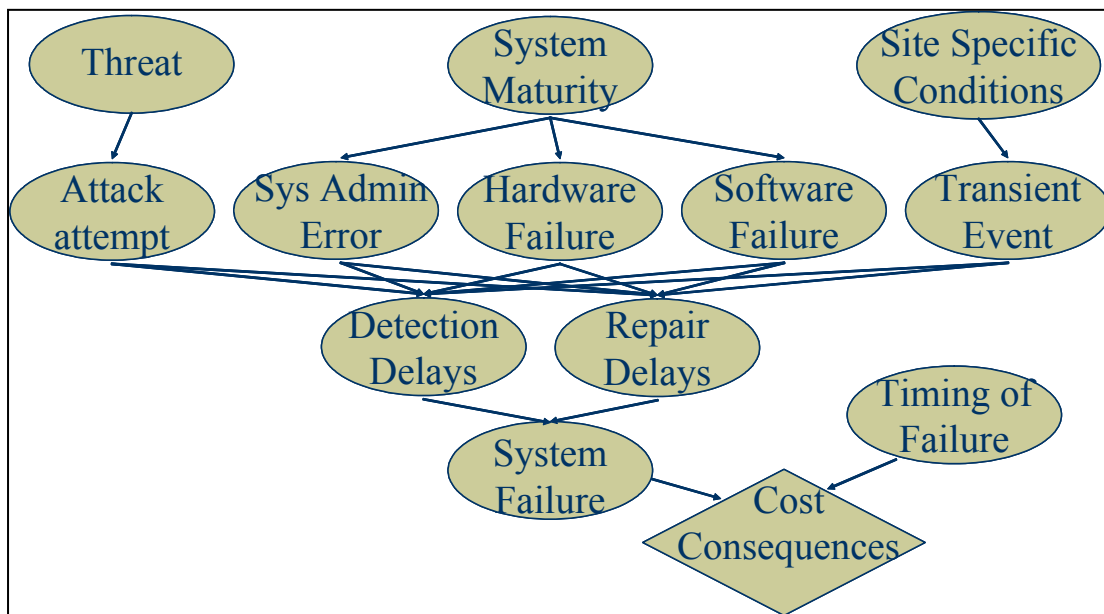


Figure 2- Influence Diagram Showing the Initiating Events and Risks to System Failure

Assume that the organization estimates that the relative costs of security losses are as follows: 17% of losses from viruses (in terms of productivity), 71% of losses from unauthorized internal logical (rather than physical) access from fraud, and 12% for all other types.¹ The magnitude of

¹ This example is loosely based on some analysis work performed to evaluate an information security program at the Dept. of Veterans Affairs. The work is documented in *Information Technology Performance Management: Measuring IT's Contribution to Mission Results*, IT Performance Management Subcommittee, Federal CIO Council, September 2001. The authors did not participate in the original analysis.

losses is estimated between \$1.1 billion and \$2.4 billion (assume a uniform distribution). In order to reduce fraud costs, the organization is planning on implementing a Public Key Infrastructure (PKI). The PKI is a combination of software, hardware, and procedures that provide secure and confidential data transfer using cryptography. The costs for an organization wide roll-out are about \$1.8 million annually. Implementing organization-wide is expected to reduce fraud incidents by 0.11%. Also, assume that users will be inconvenienced in one out of every ten-thousand transactions from failures of certifying authorities, expired keys, or corrupted keys (assume 100,000 transactions per day and an inconvenience cost of \$100 per incident). In rolling out the PKI, the organization has two alternatives: 1) organization-wide or 2) targeted. In a targeted roll-out, it is estimated that providing PKI to a key fraction of the users (50%) will cost 65% of the total cost, and will achieve 60% of the fraud avoidance benefits. For convenience, we assume that either budget is within resources available. Should PKI be implemented organize-wide or targeted?

Investing in the system organization-wide will reduce the probability of a technical failure by 0.11% which results in an expected loss reduction of \$1.925 million. To quantify the decision maker's utility, we assume a linear function measurable in dollars. Organization-wide inconveniences based on the assumed data are \$365,000 per year. Thus for the organization-wide alternative, the expected costs (implementation plus inconvenience) exceed the expected benefits by \$240,000 and for the limited implementation, the corresponding value is \$197,500. Therefore, based on the technical and security risks and benefits and assuming an expected value decision maker, the best alternative is the limited implementation.

Current State of the Project and Conference Presentation

This example is a simple illustration of the types of data needed and the approach described by the proposed framework to examine risk tradeoffs. The primary benefit of it is that it provides a proactive approach to resource management and risk identification. The research will continue with a series of case studies applying the framework to actual information systems development decisions, and in the conference presentation, we will explain the results of these case studies.

REFERENCES

- Alter, S. and M. Ginzberg, "Managing Uncertainty in MIS Implementation," *Sloan Management Review*, Fall 1978, pp. 23-31.
- Barki, H., Rivard, S., and J. Talbot, "An Integrative Contingency Model of Software Project Risk Management," *Journal of Management Information Systems*, Spring 2001, Vol. 17, No. 4, pp. 37-69.
- Barki, H., Rivard, S., and J. Talbot, "Toward an assessment of software development risk," *Journal of Management Information Systems*, 10 (1993), pp. 203-223.
- Boehm, B.W. "Software Risk Management: Principles and Practices," *IEEE Software*, January 1991, pp. 32-41.
- Cule, P., Schmidt, R., Lyytinen, K., and M. Keil, "Strategies for heading off IS project failure," *Information Systems Management*, Spring 2000, pp. 65-73.
- Denning, Dorothy, *Information Warfare and Security*, Boston: Addison-Wesley, 1999.
- Dillon, R.L., Paté-Cornell, M.E., and Guikema, S., "Programmatic Risk Analysis for Critical Engineering Systems under Tight Resource Constraints" *Operations Research*, in press.
- Fontana, J., "Net access denied: Web shutdown cripples the Department of the Interior," *Network World*, July 8, 2002, p. 51.
- Greenstein, M. and T.M. Feinman, *Electronic Commerce: Security, Risk Management, and Control*, Boston: Irwin McGraw-Hill, 2000.
- Henley, E. and H. Kumamoto: *Probabilistic Risk Assessment: Reliability Engineering, Design, and Analysis*. New York: IEEE Press, 1992.
- Keil, M., Cule, P., Lyytinen, K., and R. Schmidt, "A framework for identifying software project risks," *Communications of the ACM*, Vol. 41, No. 11, November 1998, pp. 76-83.
- Lyytinen, K., Mathiassen, L., and J. Ropponen, "Attention shaping and software risk – a categorical analysis of four classical risk management approaches," *Information Systems Research*, Vol. 9, No. 3, Sept 1998, pp. 233-255.
- Lyytinen, K., Mathiassen, L., and J. Ropponen, "A framework for software risk management," *Journal of Information Technology*, 11 (1996), pp. 275-285.
- Jiang, J. and G. Klein, "Software development risks to project effectiveness," *The Journal of Systems and Software*, 52 (2000), pp. 3-10.
- Jiang, J.J., Klein, G., and Discenza, R., "Information System Success as Impacted by Risks and Development Strategies," *IEEE Transactions on Engineering Management*, 48 (2001), pp. 46-55.
- McFarlan, F.W., "Portfolio Approach to Information Systems," *Harvard Business Review*, Sept/Oct 1981, pp. 142-150.
- Nidumolu, S.R., "The effect of coordination and uncertainty on software project performance: residual performance risk as an intervening variable," *Information Systems Research*, 6, 3 (Sept. 1995), pp. 191-219.
- Nidumolu, S.R. "A comparison of the structural contingency and risk-based perspectives on coordination in software development projects," *Journal of Management Information Systems*, 13, 2 (Fall 1996), pp. 77-113.
- Ropponen, J. and K. Lyytinen, "Can software risk management improve system development: an exploratory study," *European Journal of Information Systems*, 6 (1997), pp. 41-50.

Ropponen, J. and K. Lyytinen, "Components of Software Development Risk: How to Address Them? A project manager survey," *IEEE Transactions on Software Engineering*, Vol. 28, No. 2, Feb. 2000, pp. 96-112.

Saarinen, T, "System development methodology and project success: an empirical assessment of situational approaches," *Information and Management*, 19 (1990), pp. 183-193.

Schmidt, R., Lyytinen, K., Keil, M., and P. Cule, "Identifying Software Project Risks: An International Delphi Study," *Journal of Management Information Systems*, Spring 2001, Vol. 17, No. 4, pp. 5-36.

The Standish Group, *1998 Chaos Report*, Dennis, Mass., 1998.

Whitten, J.L., and L.D. Bentley, *Systems Analysis and Design Methods, Fourth Edition*, Irwin McGraw-Hill, 1998.