11 TOWARD AN INTEGRATED THEORY OF IT-RELATED RISK CONTROL

M. Lynne Markus
Claremont Graduate University
U.S.A.

1. Introduction

In business today, awareness of risk is growing, and risk management is increasingly seen as a critical practical discipline (Teach 1997). Further, risk is being defined broadly to include *anything* that could have a significant negative effect on the business.

For example, Microsoft recently began an integrated approach to risk management (Teach 1997). Twelve categories of business risk were identified, including financial, operational, people, and political risks (see Figure 1). Having identified these risks, Microsoft set about mapping them on several dimensions, such as potential frequency of loss producing event, potential severity, and adequacy of insurance. This analysis revealed that less than 50% of Microsoft's total business risk was adequately covered—an insight that led to the development of more effective risk management plans.

In the field of Information Systems, there has long been an interest in the risks associated with information systems and technology (Davis and Olson 1985; McFarlan 1988). However, as a field, we have not taken an integrated approach to the identification, analysis, and management of IT-related risk. By failing to do so, we are missing an important opportunity to make a major contribution in an area of pressing business need.

In this paper, I first show that our field's approach to the topic of IT-related risk has been quite fragmented, and I make the case that business people need a more integrated view of the topic. Next, I discuss some issues that help frame a theoretical perspective on IT-related risk. Finally, I examine some efforts at conceptual integration and show where they need bolstering for an integrated framework of IT-related risk management.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35505-4_33

R. Baskerville et al. (eds.), *Organizational and Social Perspectives on Information Technology*

1. Business partners (inderdependency, confidentiality, cultural conflict, contractual risks, etc.)
2. Competitive (market share, pricing wars, industrial espionage, antitrust allegations, etc.)
3. Customer (product liability, credIT-related risk, poor market timing, inadequate customer support, etc.)
4. Distribution (transportation, service availability, cost, dependence on distributors, etc.)
5. Financial (foreign exchange, portfolio, cash, interest rate, etc.)
6. Operations (facilities, contractual risks, natural hazards, internal processes and controls, etc.)
7. People (employees, independent contractors, training, staffing adequacy)
8. Political (civil unrest, war, terrorism, enforcement of intellectual property rights, change in leadership, revised economic policies, etc.)
9. Regulatory and legislative (export licensing, jurisdiction, reporting and compliance, environmental, etc.)
10. Reputational (corporate image, brands, reputations of key employees, etc.)
11. Strategic (mergers and acquisitions, joint ventures and alliances, resource allocation and planning, organizational agility, etc.)
12. Technological (complexity, obsolescence, the year 2000 problem, workforce skill sets, etc.)

Figure 1. Microsoft's 12 Categories of Business Risk (Source: Teach 1997, p. 71)

2. IT-related Risk in the IS Literature and in Business Practice

The IS field has provided many useful insights for IS professionals and business managers in the domain of IT-related risks. Many individual types of IT-related risk have been isolated and studied, although they are not always labeled as risks. For example, there is a sizable IS literature on the topic of IS *project failure* (Keil 1995; Lyytinen and Hirschheim 1987; Sauer 1993). IS project failure can usefully be categorized as an IT-related risk, but it is only one of many. Other IT-related risks include *operational failure* or lack of reliability (Markus and Tanis 2000), *security breaches* (Baskerville 1993; Straub and Nance 1990; Straub and Welke 1998), *reputational damage* to a company owing to its failure to safeguard the privacy of customer data (Smith 1994), and *strategic risk* (Vitale 1986), such as adopting a new IT too soon or too late.

In general, IS research on risks falls into two broad categories: (1) risks related to the *development* of information systems and (2) risks related to the ongoing *operation* of information systems. This grouping of IT-related risks mirrors the way such risks are managed in practice by IS professionals. Most IS organizations structurally separate applications development from operations. In some cases, application development

reports directly to business units, while operations reports to the CIO. Thus, the separate frameworks developed for managing project risks (Keil 1995) versus operational risks (Straub and Welke 1998) meet the needs of the different categories of IS professionals engaged in these tasks.

The major exception to the general statement that the academic treatment of IT-related risks is fragmented into discrete investigations of a variety of project and operational risks is Peter Neumann's (1995) treatise on *Computer-Related Risks* compiled from the Internet newsgroup, *The Risks Forum*, that Neumann has moderated for years. Neumann justly refers to his work as integrated treatment of computer-related risks, and I will discuss this work more later, but it is more properly viewed as a Computer Science contribution than a work in the Information Systems tradition.

However well the divergent approach to studying IT-related risks fits current IS practice, it is disadvantageous *from the perspective of the executive leadership of companies making major investments in information technology*. Executives tend to become involved in critical IT decision making only when new IS development or enhancement projects are initiated. They rarely become involved in IT operational issues unless there has been a significant problem, such as a major operational failure or a serious security breach. Thus, executives tend to be distanced from making decisions concerning operational IT-related risks. Integrated frameworks for IT investment decision making that combine benefits, costs, and both development and operational risks could help ensure better decisions from an organization-wide perspective.

From the business point of view, dividing the management of IT-related risk into development risk and a collection of disparate operational risks is counterproductive. Businesses should think of their IT initiatives as investments that are intended to pay off over their entire lifecycles. While it is true that the nature of IT-related risk changes as an IT investment progresses through its lifecycle, an integrated approach to IT-related risk management allows for intelligent tradeoffs between development costs and risks on the one hand and operational costs and risks on the other. Lack of an integrated approach to IT-related risk management makes possible the situation in which decisions designed to *reduce* project cost and schedule risk (e.g., ignore control needs, shortcut training and testing, etc.) may actually *increase* the operational risks of non-use, external threat, and contingencies.

The case of the Fox-Meyer Drug Company provides a useful illustration of how companies can suboptimize total business risk while attempting to manage project metrics. When Fox-Meyer Drug chartered its ERP system implementation, the CIO was aware that it was a "bet your business" proposition (Bulkeley 1996). Yet, the $60 million project was approved at the same time that the company also embarked on a state-of-the art $18 million automated warehouse. During the Project Phase, bad luck intervened: Fox-Meyer Drug lost a large customer, accounting for 15% of its business. To increase revenues, the company aggressively bid on new business: they figured contract pricing on the assumption that the projected annual $40 million savings from the SAP project would be realized immediately on startup, and they decided to advance the SAP rollout by 90 days. That close to the end of the project, little was left to do other than training and testing. So project team members decided not to test modules that had not been customized (thus failing to detect configuration errors). Cutover to the new system resulted in disaster. Meanwhile, the automated warehouse also did not perform as

planned. It was estimated that the company sustained an unrecoverable loss of $15 million from erroneous shipments. The company was forced into bankruptcy and shareholders have since sued both the enterprise systems vendor and the integration consultant for $500 million each.

In this example, there are multiple, interacting factors in the failure. Some of them lay within the company's control, others did not. But the example clearly shows that decisions made to address development issues can have much wider consequences. One wonders whether Fox-Meyer's executives would have been so willing to advance the project schedule if they had taken a serious look at the likelihood and consequences of operational failure owing to poor project testing.

Today, in the business world, there is much discussion of "TCO," the total cost of ownership of IT systems. The TCO concern first arose in the context of standalone PCs (Strassmann 1990). But the TCO issue has acquired special significance in the context of packaged enterprise resource planning (ERP) software. Initially, executives focused only on the sizable license costs of this software. Later, they learned that ERP software license costs often pale in comparison with the costs of configuration consulting, technical platform, end-user training, and maintenance. Today, it is generally considered best business practice for executives to consider both the total lifecycle costs and the total lifecycle benefits of an IT investment. Should not the third major component of an executive's IT investment decision making be *total lifecycle risks,* where this concept comprises both project and operational risks?

An integrated approach to the management of IT-related risk is especially important in the current era for two reasons. First, worldwide connectivity through the Internet increases the opportunities for widespread fraud and cascading operational failure. Second, organizations are increasingly relying on outside parties for the development, operation, and management of their information systems. One could argue that IT-related risk management (ensuring investment payoff, while controlling potential negative consequences) is the *only* IT job an organization has left in an environment of total outsourcing.

3. Framing the Discussion of IT-related Risk

An integrated approach to IT-related risk must start with basic definitions. In this section, I define IT-related risk, present a typology of IT-related risks, discuss the issue of stakeholders—whose goals are to be served?—and outline the academic case for an integrated approach to this important topic.

3.1 What is IT-related Risk?

A significant obstacle in the way of an integrated approach to IT-related risk is definitional: what is the appropriate level of analysis of IT-related risk? And what is risk?

Discussions of IT-related risk often take a computer-based information system—a technical artifact—to be the appropriate level of analysis for the study of risk. Certainly, important technical issues, such as the existence of "trap doors" in software or the

vulnerability of much modified code, must be addressed in any complete treatment of IT-related risks. However, the perspective I am advocating in this article suggests that there is need for an integrated treatment of IT-related risks at the organizational and interorganizational levels of analysis. At the organizational level, the knowledge and skills of users and their social interactions while using computer-based information systems are as important to an understanding of risk as is the technical system itself. Since so many of today's most interesting IT developments involve "business-to-business" and "business-to-consumer" e-commerce, it is often necessary to extend an analysis of risks beyond the boundaries of a single organization.

Different connotations and definitions of IT-related risk can be found in the literature and in common usage. One common definition holds risk to be uncertainty; alternatively, a risk is a wager (or an attempt at rewards). A second definition considers risk to be the possibility of loss. A third definition views risk as a negative quality of an opportunity that must be effectively managed.

These definitions of risk reflect very different emotional stances toward risk and its management. Someone who views risk as a wager for potential benefits to be maximized is likely to approach risk management quite differently than someone who views risk as the possibility of loss to be minimized. For my purposes here, I choose the third definition, because my focus is on managing the business risks associated with investments in information technology. At the same time, I am aware that risk is an emotionally difficult topic, because some people approach risks avidly, some people avoid thinking about them, and still others consider them emotionally neutral and completely amenable to rational analysis.

> IT-related risk is the likelihood that an organization will experience a significant negative effect (e.g., technical, financial, human, operational, or business loss) in the course of acquiring, deploying, and using (i.e., maintaining, enhancing, etc.) information technology either internally or externally (i.e., facing customers, suppliers, the public, etc.)

3.2 What Kinds of IT-related Risk Are There?

An additional obstacle in the way of an integrated treatment of IT-related risk is that many things one might label as risk have been discussed in the IS literature under other names. For example, the IT project failures literature rarely uses the label of "risk." A few authors (Clemons 1995; Lyytinen and Hirschheim 1987) have proposed typologies of IT-related risk. Building on their efforts and drawing on a wide range of literature, I propose the following 10 categories of IT-related risk:

1. Financial risk (the technology costs more than expected, yields fewer financial benefits, etc.)
2. Technical risk (the technology used is immature, poorly understood, unreliable, obsolete, etc.)

3. Project risk (the project is late, there is turnover of key personnel, the project becomes a "runaway," etc.)
4. Political risk (the project/system/technology is subject to political infighting or resistance)
5. Contingency risk (accidents, disasters, viruses, etc.)
6. Non-use, underuse, misuse risk (the intended users do not use the technology, they do not use it sufficiently or in a manner that would lead to the intended benefits, inappropriate use, etc.)
7. Internal abuse (malicious or felonious destruction, theft, abuse, etc., by company insiders)
8. External risk (hacking, theft of assets, willful destruction, etc., by company outsiders)
9. Competitive risk (negative reactions by customers, competitors, suppliers, etc., to the company's IT initiatives)
10. Reputational risk (negative reactions by the public at large, the media, the government, etc., to a company's IT initiatives)

In short, IT-related risk includes *anything* related to IT that could have significant negative effects on the business or its environment from the perspective of an executive investing in IT.

3.3 Who Are the Stakeholders in IT-related Risk?

It should be clear from the preceding discussion that there are many stakeholders where IT-related risk is concerned. Inside the focal company, stakeholders include executives, IS applications developers, IT infrastructure maintainers, and many different types of users. External to the company are customers, business partners, the public at large, investors, regulators, competitors, and others. These many stakeholders have widely differing interests in the risks of IT systems and their interests are likely to conflict often.

This paper proposes an integrated view of IT-related risks from the perspective of an executive decision maker, not because I think that executives are smarter, more ethical, or more important than other stakeholders. Instead, I am arguing that it is in the best interests of rational, well-informed executive decision makers to manage the total lifecycle risks of IT investments, regardless of who might be most affected by the risks. Given the fragmentation of IS practice into development versus operational concerns, it is not likely that IS professionals are as well placed as organizational executives to manage the full spectrum of IT-related risks. I hasten to add, however, the IS professionals are essential *partners* in the effective management of IT-related risk.

3.4 The Academic Case for an Integrated Approach to IT-related Risk Management

Here and there, academics have called for an integrated treatment of IT-related risk. The most comprehensive argument is that of Neumann, whose focus encompasses security,

reliability, safety, privacy, and other operational risks. Writing on the need for an integrated treatment of security and reliability, for example, Neumann notes:

> Considerable commonality exists between reliability and security. Both are weak-link phenomena. For example, certain security measures may be desirable to hinder malicious penetrators, but do relatively little to reduce hardware and software faults. Certain reliability measures may be desirable to provide hardware fault tolerance, but do not increase security. On the other hand, properly chosen system architectural approaches and good software engineering practice can enhance both security and reliability. Thus, *it is highly advantageous to consider both reliability and security within a common framework*, along with other properties such as application survivability and application safety. [Neumann 1995, pp. 129-130, emphasis added]

In the IS system failure literature, there is widespread recognition that development and implementation/use issues must be jointly considered. For example, Lyytinen and Hirschheim discuss both development failures and use failures (i.e., failure in operation) and argue that different failure types must be addressed in a common framework. Markus and Keil (1994) and Markus and Tanis make similar points.

In the area of IS security, Baskerville makes a compelling case for an integrated approach to system development and the management of operational IT security risks. By tracing the evolution of system development and security management methods, he shows that initially there was no integration. Gradually, security risk analysis and management procedures have become built into system development methods. By extension, management of all other IT-related risks listed earlier in this paper should also be incorporated in system development methods.

In short, here and there in the literature, it is possible to find arguments that, when assembled, call for an integrated approach to the management of IT-related risk. Such an approach would encompass both project failure and a range of operational risks, including those related to safety, reliability, security, privacy, non-use, and reputation.

4. Theoretical Perspectives on IT-related Risk and Risk Control

Since Neumann claims to have taken an integrated approach to computer-related risks, what more needs to be done? Cannot the IS field simply adopt Neumann's framework and declare the problem solved?

On the contrary, I argue that, while Neumann's work is an important first step toward an integrated theory of IT-risk and risk management, it is lacking in a number of areas that require theoretical integration. Those areas are the social psychological dimensions of risk perception, the structural conditions of risk management, the dynamics of risk control, and the dynamics of risk.

4.1 Social Psychological Dimensions of Risk Perception

Neumann does a thorough job of treating the various system-related causes, both accidental and intentional, of computer-related disasters. While he includes a chapter on "the human element," this chapter falls far short of capturing the social-psychological processes that go into the human side of the equation. Notably absent from his discussion is the phenomenon of "escalating commitment" to a losing course of action that has proved so useful in analyzing certain IS project failures (Keil 1995; Staw 1993). Also lacking is a treatment of the many cognitive biases that are known to affect people's judgment in making decisions involving risk (Sitkin and Pablo 1992), in dealing with crises (Pearson and Mitroff 1993), and in problem solving in complex situations (Dörner 1989). For a wonderful complement on the human side to Neumann's technology-oriented analysis, see Dörner.

4.2 Structural Conditions of Risk Management

A second area in which Neumann's analysis of computer-related risks needs augmentation for the IS domain is that of the structural conditions in which IT-related risk is created and materializes into problems. Structural conditions are the social and economic arrangements (e.g., reporting relationships and policies) that influence the processes and outcomes of IS work (Orlikowski 1992). Examples of relevant structural conditions include the separation of development from operations work in many IS departments and the outsourcing of selected IT-related tasks to consultants and vendors. Neumann discusses large programming projects as a human source of risk, but he says nothing about how variations in the organization and management of such projects might contribute to the incidence or control of risks.

4.3 Dynamics of Control

A third area in which Neumann's analysis of computer-related risks needs enhancement is that of the dynamics of risk *control* strategies. Neumann devotes an entire chapter to strategies for controlling risk, such as modeling and simulation, complexity management, reliability improvement approaches, and so forth. Interestingly, while his analysis of computer-related risks is quite holistic, his approach to risk control is not: it is in essence a laundry list of techniques and rules of thumb. He does not attempt an integrated methodology of system engineering for the prevention of risk nor tackle the issue of how to recover from failure. He also does not tackle the difficult problem of ensuring that people follow acceptable methodologies (hence the importance of understanding the structural conditions under which IS work gets done).

An integrated theory of risk control needs to address what is known about the different types of strategies for gaining and maintaining control over people and organizational processes. Review of the control literature suggests that the types of control potentially useful in managing IT-related risk are as varied as the risks themselves (Handy 1995; Simons 1995a, 1995b). For example, Straub and Welke identify four

distinct, sequential activities involved in the management of systems security risks: deterrence, prevention, detection, and recovery. Combining these sources, a list of risk control strategies would surely include the following:

1. Plans (e.g., backup, disaster recovery, etc.)
2. Policies (e.g., regarding unauthorized use of a company's computer resources, etc.)
3. Operational controls (e.g., budgets, performance evaluations, etc.)
4. Automated controls (e.g., passwords, access monitoring, etc.)
5. Physical controls (e.g., cardkeys, etc.)
6. Audit and detection (e.g., post project audits, system penetration detection, etc.)
7. Risk awareness building (e.g., training, bulletins, etc.)
8. Belief systems (e.g., beliefs about value of customer privacy, etc.)
9. Social systems (e.g., behavioral norms and reminders about confidentiality, etc.)

Further, the control literature suggests that control attempts are not invariably successful. While it is generally recognized that too little control is bad, a sizable body of literature suggests that too much control is also bad. Too much control has been associated with three types of negative consequences. First, too much control is expensive. In fact, the high cost of control is a major reason given for reengineering business processes with looser control (Sia and Neo 1997). Second, too much control can interfere with business operation and flexibility and can damage the relationship between controllers and controllees (Block 1993). Third, too much control is associated with unintended human and social consequences (Handy 1995; Sitkin and Roth 1993). These negative consequences include low morale and circumventing the rules; ironically, excessive control can also promote fraud. There is a science of control, just as there is a science of technology failure, and an integrated theory must incorporate both.

4.4 Dynamics of Risk

As we move toward an integrated theory of IT-related risk and risk management, it is important to keep in mind the empirical evidence about how problems, crises, and disasters materialize from risk. Studies of nuclear power plant accidents (Perrow 1984) and IT-related accidents (Neumann 1995) show that crises, disasters, and failures often have multiple independent or correlated causes. These "weak link" phenomena remind us that we should not take a static view of risk but should recognize that risk is a dynamic function of technology developments and human interventions.

The literature on IT project risk often appears to assume that risk is greatest at the start of the project when the unknowns are greatest, then decreases over the life of the project as work progresses toward completion. This view suggests that risk does not remain static, but changes as a function of prior decisions and behavior. Therefore, one can posit the concept of "residual risk" that varies throughout a project (Nidumolu 1995) and by extension throughout the lifecycle of a system.

Residual risk is often assumed to decrease monotonically over the life of IT projects; but, in the IT domain, one must consider the possibility that residual risk will actually

increase over a system's lifecycle. In the first place, as systems age, they are maintained and enhanced; over time, this process increases their fragility or failure-proneness (Lientz and Swanson 1980). (This is why there is such a strong emphasis on development for maintainability, another example of the need for an integrated risk management approach.) Further, there is an increasing trend toward the integration of formerly discrete systems. As systems are integrated with other systems, complexity and tight-coupling increase the chances of failure (Neumann 1995; Perrow 1984). For example, in a recent project involving the implementation of SAP R/3 financials, Microsoft loaded financial data into a data warehouse and provided access to the data and preformatted reports via the corporate intranet. Integration of SAP R/3 with data warehousing and intranet technology vastly increased the number of people who had access to financial data and vastly increased the risks of non-use, internal abuse, external risk, etc. (Bashein, Markus, and Finley 1997).

An additional consideration is the actions people take to remedy problems that arise as projects and systems pass through their lifecycles. In situations involving system development and operation (as in the progression of a nuclear power plant incident), people may misdiagnose the causes of problems and apply attempted solutions that actually make the situation worse (Markus and Tanis 2000). They thus create new situations that call forth additional actions and changes (Orlikowski 1996). Therefore, an integrated theory of IT-related risks must also take into account the second-order consequences of human problem-solving behavior.

5. Conclusion

Much of the research in the IS field deals directly or indirectly with issues of IT-related risk, although that term is seldom used. The business world is beginning to see the value of an integrated approach to identifying and managing business risk; the time is right for the IS field to begin developing an integrated approach to identifying and managing IT-related risk. Not only will such an approach be useful to businesses in their attempts to obtain maximum value from their IT investments, it will also help bring together a large part of the IS literature under a common conceptual umbrella. By viewing system development and maintenance along with package acquisition and outsourcing as part of the business's IT investment process, risk management becomes the center of attention. By viewing system development failure, security breaches, and competitive threats as different types of the unitary phenomenon of IT-related risk, it becomes possible to make intelligent end-to-end tradeoff decisions throughout the lifecycles of systems in organizations.

References

Bashein, B. J., Markus, M. L., and Finley, J. B. *Safety Nets: Secrets of Effective Information Technology Controls*. Morristown, NJ: Financial Executives Research Foundation, Inc., 1997.

Baskerville, R. "Information Systems Security Design Methods: Implications for Information Systems Development," *ACM Computing Surveys* (25:4), 1993, pp. 375-414.

Block, P. *Stewardship: Choosing Service Over Self-Interest.* San Francisco: Berrett-Koehler Publishers, 1993.

Bulkeley, W. M. "A Cautionary Network Tale: Fox-Meyer's High-Tech Gamble," *Wall Street Journal Interactive Edition*, November 18, 1996.

Clemons, E. K. "Using Scenario Analysis to Manage the Strategic Risks of Reengineering," *Sloan Management Review* (36:4), 1995, pp. 61-71.

Davis, G., and Olson, M. *Management Information Systems: Conceptual Foundations, Structure and Development.* New York: McGraw-Hill, 1985.

Dörner, D. *The Logic of Failure: Recognizing and Avoiding Error in Complex Situations.* Reading, MA: Addison-Wesley, 1989.

Handy, C. "Trust and the Virtual Organization," *Harvard Business Review* (73:3), 1995, pp. 40-50.

Keil, M. "Identifying and Preventing Runaway Systems Projects," *American Programmer* (8:3), 1995, pp. 16-22.

Lientz, B. P., and Swanson, E. B. *Software Maintenance Management: A Study of the Maintenance of Computer Applications in 487 Data Processing Organizations.* Reading, MA: Addison-Wesley, 1980.

Lyytinen, K., and Hirschheim, R. "Information Systems Failures: A Survey and Classification of the Empirical Literature," in *Oxford Surveys in Information Technology*, P. I. Zorkoczy (ed.), 4. Oxford: Oxford University Press, 1987, pp. 257-309.

Markus, M. L., and Keil, M. "If We Build It They Will Come: Designing Information Systems That Users Want To Use," *Sloan Management Review*, Summer, 1994, pp. 11-25.

Markus, M. L., and Tanis, C. "The Enterprise Systems Experience-From Adoption to Success," in *Framing the Domains of IT Research: Glimpsing the Future Through the Past*, R. W. Zmud (ed.). Cincinnati, OH: Pinnaflex, 2000.

McFarlan, F. W. "Portfolio Approach to Information Systems," *Harvard Business Review* (59:5), 1988, pp. 142-150.

Neumann, P. G. *Computer Related Risks.* New York: The ACM Press, 1995.

Nidumolu, S. "The Effect of Coordination Uncertainty on Software Project Performance: Residual Performance Risk as an Intervening Variable," *Information Systems Research* (6:3), 1995, pp. 191-219.

Orlikowski, W. J. "The Duality of Technology: Rethinking the Concept of Technology in Organizations," *Organization Science* (3:3), 1992, pp. 398-427.

Orlikowski, W. J. "Improvising Organizational Transformation Over Time: A Situated Change Perspective," *Information Systems Research* (7:1), 1996, pp. 63-92.

Pearson, C. M., and Mitroff, I. I. "From Crisis Prone to Crisis Prepared: A Framework for Crisis Management," *The Academy of Management Executive* (7:1), 1993, pp. 48-59.

Perrow, C. *Normal Accidents: Living With High-Risk Technologies.* New York: Basic Books, 1984.

Sauer, C. *Why Information Systems Fail: A Case Study Approach.* London: McGraw-Hill, 1993.

Sia, S. K., and Neo, B. S. "Reengineering Effectiveness and the Redesign of Organizational Control: A Case Study of the Inland Revenue Authority of Singapore," *Journal of Management Information Systems* (14:1), 1997, pp. 69-92.

Simons, R. "Control in an Age of Empowerment," *Harvard Business Review* (73:2), 1995a, pp. 80-88.

Simons, R. *Levers of Control: How Managers Use Innovative Control Systems to Drive Strategic Renewal.* Boston: Harvard Business School Press, 1995b.

Sitkin, S. B., and Pablo, A. L. "Reconceptualizing the Determinants of Risk Behavior," *Academy of Management Review* (17:1), 1992, pp. 9-38.

Sitkin, S. B., and Roth, N. L., "Explaining the Limited Effectiveness of Legalistic 'Remedies' for Trust/Distrust," *Organization Science* (4:3), 1993, pp. 367-392.

Smith, H. J. *Managing Privacy: Information Technology and Corporate America.* Chapel Hill, NC: The University of North Carolina Press, 1994.

Staw, B. M. "Organizational Escalation and Exit: Lessons From the Shoreham Nuclear Power Plant," *Academy of Management Journal* (36:4), 1993, pp. 701-732.

Strassmann, P. A. *The Business Value of Computers: An Executive's Guide.* New Cannan, CT: The Information Economics Press, 1990.

Straub, D. W., and Welke, R. J. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4), 1998, pp. 441-469.

Straub, D. W., and Nance, W. D. "Discovering and Disciplining Computer Abuse in Organizations: A Field Study," *MIS Quarterly* (14:1), 1990, pp. 45-60.

Teach, E. "Microsoft's Universe of Risk," *CFO*, March 1997, pp. 69-72.

Vitale, M. R. "The Growing Risks of Information Systems Success," *MIS Quarterly* (10:4), 1986, pp. 327-334.

About the Author

M. Lynne Markus is Professor of Management at the Peter F. Drucker Graduate School of Management and Professor of Information Science at the School of Information Science, Claremont Graduate University. She has also taught at the Sloan School of Management (MIT), the Anderson Graduate School of Management (UCLA), the Nanyang Business School, Singapore (as Shaw Foundation Professor), and Universidade Tecnica de Lisboa, Portugal (as Fulbright/FLAD Chair in Information Systems). She began thinking about IT-related risks while conducting research for the Financial Executives Research Foundation. Lynne can be reached by e-mail at m.lynne.markus@cgu.edu.