

INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

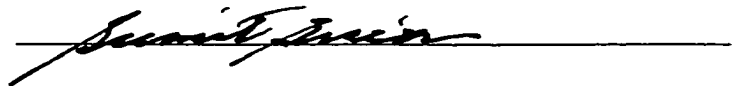
ProQuest Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
800-521-0600

UMI[®]

THE SECURITY OF THE IT RESOURCE AND MANAGEMENT SUPPORT:
SECURITY RISK MANAGEMENT PROGRAM EFFECTIVENESS

The members of the Committee approve the doctoral
dissertation of Andrew Gerald Kotulic

Sumit Sircar
Supervising Professor



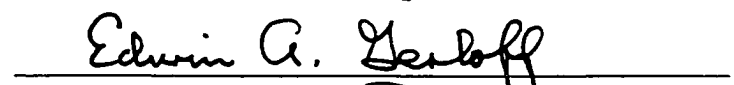
Craig W. Slinkman



David A. Gray



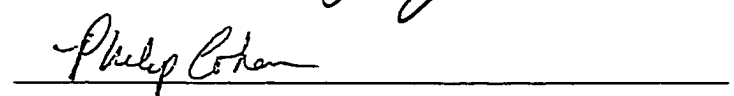
Edwin A. Gerloff



Peter Mykytyn



Dean of the Graduate School



Copyright © by Andrew Gerald Kotulic
All Rights Reserved

THE SECURITY OF THE IT RESOURCE AND MANAGEMENT SUPPORT:
SECURITY RISK MANAGEMENT PROGRAM EFFECTIVENESS

by

ANDREW GERALD KOTULIC

Presented to the Faculty of the Graduate School of
The University of Texas at Arlington in Partial Fulfillment
of the Requirements
for the Degree of
DOCTOR OF PHILOSOPHY

THE UNIVERSITY OF TEXAS AT ARLINGTON

May 2001

UMI Number: 3010038

Copyright 2001 by
Kotulic, Andrew Gerald

All rights reserved.

UMI[®]

UMI Microform 3010038

Copyright 2001 by Bell & Howell Information and Learning Company.

All rights reserved. This microform edition is protected against
unauthorized copying under Title 17, United States Code.

Bell & Howell Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

ACKNOWLEDGMENTS

My dissertation committee chair, Dr. Sumit Sircar, deserves special thanks for never giving up on me during the convoluted trip associated with producing this manuscript. He was always willing to listen to what the latest roadblock was and how I was planning to get around it. He usually had advice about how I might be able to minimize the number of speed bumps and chuckholes on a selected detour and keep moving ahead.

My thanks to the committee members, Drs. Edwin A. Gerloff, David A. Gray, Peter Mykytyn, and Craig W. Slinkman. They each contributed their own special talents so that the quality of the manuscript wasn't compromised during the many, many detours that had to be taken during the trip. Additionally, my thanks go to the two colleagues that were willing to answer my telephone calls and listen to me about the size of the chuckholes and the height of the speed bumps I had encountered on the latest detour. The seven were a great pit crew.

March 30, 2001

ABSTRACT

THE SECURITY OF THE IT RESOURCE AND MANAGEMENT SUPPORT: SECURITY RISK MANAGEMENT PROGRAM EFFECTIVENESS

Publication No. _____

Andrew Gerald Kotulic, Ph.D.

The University of Texas at Arlington, 2001

Supervising Professor: Sumit Sircar

The exploratory research study addressed the issues required to provide a theoretically based model that could be developed and validated to study the process that leads to effective Security Risk Management (SRM) programs. The model incorporates desired expectations in an IS area outside of the EUC domain and includes a direct relationship between executive management support and SRM program effectiveness. Additionally, the study followed suggested procedures to develop valid, reliable research instruments in order to empirically capture the dimensions of an original SRM Program posture construct included in the conceptual model.

The research study used a mail survey research methodology partially based on “The Tailored Design Method” to solicit responses from 1,500 major U.S. business organizations across a wide range of SICs. The responses were to be used to test a series of hypotheses in order to understand the relationships between variables in the process that leads to effective SRM programs. Additionally, the study includes a section describing the results of gathering responses from the firms that would not respond to the original research study.

TABLE OF CONTENTS

ACKNOWLEDGMENTS	iv
ABSTRACT	v
Chapter	
I. OVERVIEW OF THE RESEARCH PROBLEM AND THE RESEARCH STUDY	1
II. LITERATURE REVIEW, CONCEPTUAL RESEARCH MODEL AND RESEARCH HYPOTHESES	24
III. ORIGINAL RESEARCH STRATEGY AND METHODOLOGY	66
IV. REVISED RESEARCH STRATEGY AND RESPONSE RATES	90
V. ANALYSIS AND INTERPRETATION	100
VI. CONTRIBUTIONS AND RECOMMENDATIONS	118
TABLES	124
Appendix	
A. RESEARCH SURVEY INSTRUMENTS	152
B. RESEARCH STUDY LETTERS	178
REFERENCES	183
BIOGRAPHICAL STATEMENT	215

LIST OF FIGURES

Figure	Page
1. Theoretical Model of Security Concerns	35
2. Conceptual Model of SRM Program Effectiveness	39
3. A Conceptual Model for User Information Satisfaction	40
4. A Discrepancy Model of End-User Desires	41
5. Alternative Models of Executive Source	42
6. Original Research Model SRM Program Effectiveness	67
7. Revised Research Model SRM Program Effectiveness	68
8. Suggested Procedures for Developing Better Measures	69

LIST OF TABLES

Table	Page
1. List of Accidental and Intentional Threats to Information	125
2. Components of a Security Risk Management Program	126
3. Definitions of Constructs and Dimensions	128
4. Research Constructs, Dimensions and Measures Used in the Data Collection Phase	131
5. Pilopt Test Firm Data	133
6. Response Rates	134
7. Non Response Feedback from 74 Firms	135
8. IT Resource Posture Strategic Integration	136
9. IT Resource Posture Electronic Integration (EI) Level	137
10. IT Resource Posture Reach	138
11. IT Resource Posture Range	138
12. Business Risk Propensity	139
13. Organization Structure	139
14. Executive Management Support Involvement	140
15. Executive Management Support Participation	140
16. Security Policy Development	141
17. Security Policy Process	142
18. Security Protection Plan	143
19. Security Awareness Training and Accountability	143
20. Security Risk Management Program Effectiveness	144
21. Confirmation/Disconfirmation	145

22.	Demographic Information for All Respondents	146
23.	Demographic Information for TMT Respondents	147
24.	Demographic Information for CSW Respondents	148
25.	Demographic Information for CIO Respondents	149
26.	Demographic Information for Function Manager Respondents	150
27.	Employment History for Respondents	151

CHAPTER I
OVERVIEW OF THE RESEARCH PROBLEM
AND THE RESEARCH STUDY

1.0 Introduction

Chapter 1 contains numerous reports of security breaches due to the exploitation of vulnerabilities associated with the Information Technology (IT) resource. These reports add support for conducting research associated with what is required for effective security risk management (SRM) programs. This chapter also contains a brief evaluation of the historical development of Information Security within the context of the progressive uses of IT. The chapter also emphasizes the importance of soliciting top manager team (TMT) support and accounting for management characteristics in developing effective SRM programs. Additionally, chapter 1 contains the research questions, the research study goals, the objectives and methodology. Finally, this chapter identifies the potential limitations of the research study.

1.1 Reported Security Breaches

The growth in reported losses attributed to security breaches is staggering. In 1994 the average corporation with 1,000 PCs lost approximately \$300,000 in productivity and direct costs, through security breaches ("INFOSYS," 1996). Significant portions of these losses were due to ineffective virus prevention and eradication measures present in firm level SRM programs. In 1989 Bidgoli & Azarmsa identified computer viruses as the latest security threat U.S. firms would face as they planned for a networked IT environment. Today, their prediction has become reality with over 56,000 viruses in existence and thousands of new ones projected to be released every year (DeLong, 2001).

Nelson (1995) pinpointed mutation engines and advanced stealth techniques as the two most significant threats to microcomputers and LANs. The author attributes the reported growth rates of viruses directly to the appearance of virus toolkits. The Nelson article was typical in alerting firms to the growing security risks associated with the new generations of viruses. The next year, a National Computer Security Association estimate placed the potential business losses to U.S.-based companies at \$5 to \$6 billion in 1996 from virus-related causes (Violino, 1996). Recently, 80% of the 1,897 respondents to the 2000 Information Security Industry Survey reported that in the past 12 months they had experienced outsider security breaches from malicious code (viruses/trojans/worms). Additionally, 70% reported they had experienced insider security breaches from malicious code in the past 12 months (Briney, 2000). The projected global business losses from malicious code security breaches are reaching unbelievable levels. A recent study by Reality Research projected that \$1.5 trillion would be experienced in global business losses from malicious code security breaches in 2000 (McDonald, 2000).

Security breaches also occur due to hardware and software faults where there is little operating experience and poor physical security. In these cases SRM policy must include measures to protect against security breaches during backup, recovery and repair processes when the IT resource is most vulnerable (Axelrod, 1990). In 1996 there was a report about a "computer security glitch" that resulted in more than 800 customers of the First National Bank of Chicago receiving a total of \$763.9 billion deposited in their checking accounts. The American Bankers Association called it the largest error in the history of the U.S. Banking Industry ("Risks-Forum Digest," 1996a). In the same issue, they carried a report of a break-in at an Australian governmental building housing treasury offices. The report stated that approximately 55 computers were dismantled and the burglars removed the hard disk drives and memories. The report did not list any estimates of the potential financial loss. The report further cited a spokesperson for the Australian premier as saying that the incident resulted in a

review of security measures at all government buildings.

In 1996, the *Wall Street Journal* reported that the U.S. Senate's Permanent Investigations Subcommittee stated that in 1995 major U.S. banks and other large corporations lost an estimated \$400 million of the \$800 million lost globally due to intentional security intrusions by "computer hackers." The report contained the testimony from the head of the Computer Emergency Response team who stated, "Of 346 cases analyzed during the first quarter of this year (1996), 20% involved 'total comprises' of computer systems by hackers who gained the ability to enter most files." An official of the Computer Security Institute testifying on the results of a recent survey of corporate-security specialists stated that "of the 428 who responded, 42% reported attacks within the last year, though only 17% of these reported the incidents to law-enforcement officials" (Fialka, 1996).

The U.S. government has also been experiencing significant growth rates in security breaches. In 1996, a senate subcommittee reported that the Department of Defense (DOD) estimated that approximately 65% of the 250,000 known yearly intrusion attempts into their computer systems succeed ("Edupage," 1996a). In the same issue, the Deputy U.S. Attorney General testified before a Senate subcommittee that the United States faces "an electronic Pearl Harbor" due to the potential for electronic attacks that could disrupt or disable the hybrid public/private network information infrastructure. Today, similar reports are appearing about the penetration of DOD computer systems. In 1999 a 16-year-old successfully hacked into DOD and NASA computer networks, resulting in his being able to steal NASA proprietary software used to maintain life systems in the international space station, worth \$1.7 million. He was also able to capture 19 defense agency employee names and passwords and to penetrate a network used by a government agency involved in conventional and non-conventional warfare (Hulme, 2000).

These reported security breaches are only the tip of the iceberg relative to the potential magnitude of the financial consequences resulting from ineffective SRM programs. The

changing task environments of organizations are generating new threats and vulnerabilities that will result in a continuous rise in reported security breaches.

1.2 Recent Threats and Vulnerabilities

There are several areas reported as being major causes of rising security concerns relative to threats and vulnerabilities. Some of the areas include network security, the Internet and Intranets, competitive intelligence operatives, electronic commerce and outsourcing IS functions to foreign locations. These new threats and vulnerabilities have to be considered in developing effective SRM programs. The results of the 1998 Information Week/PricewaterhouseCoopers Global Information Security Survey highlight the point that network security and unauthorized external access were becoming major concerns of corporate IT managers. The security issues associated with network access are more complex in nature than physical security issues and require multiple tradeoffs in order to provide access to IT resources within acceptable risk levels. Major findings from the 1998 survey indicated that firms that engage in electronic business and electronic commerce were reporting three times the frequency of information loss and trade secret theft than firms that did not engage in these activities. They reported that 6% of the 1,440 firm's surveyed, who were engaged in electronic commerce, reported losses of data or trade secrets via security breaches (Dalton, 1998).

Firms that engage in electronic commerce may be more vulnerable to the growing threat of electronic fraud and extortion. The magnitude and frequency of these types of computer crimes are growing. Several recent examples include the theft of 300,000 credit card numbers from CD Universe demanding \$100,000 for returning them. A recent report in the *London Sunday Times* states that up to \$619 million U.S. has been extorted from banks in Great Britain by "computer crackers" who have penetrated their computer systems. They demanded payments and threatened to destroy the banks systems or had already crippled their systems using "logic bombs" and other advanced computer warfare techniques (Kabay & Walsh, 2000).

A 1996 report released by the U.S. General Accounting Office stated that the Department of Energy and the National Security agency estimated that more than 120 countries had computer attack capabilities. Furthermore, in a recent FBI survey, 47% of business organizations that reported unauthorized external access of their computer systems suspect that the unauthorized access was executed by a foreign government or a foreign competitor (GAO, 1996a). Jon Swartz of the *San Francisco Chronicle* summarized the data from other sections of the same survey and reported that 20% of the same 428 respondents admitted that they did not know whether they had been electronically probed or intruded. Seventy-five percent of these said that they would not report incidents because of fear of negative publicity ("Risks Digest," 1996b). The era of business organizations unknowingly and some possibly knowingly staking their corporate long-term survival on the IT resource has arrived

The use of outsourcing for systems development, programming and data processing to "cheap labor" data havens has been identified as a major security (business) risk for organizations that engaged in MIS outsourcing. The use of foreign locations similar to "Jamaica," which has been called a "security absent" environment by Madsen (1995), adds a new level of complexity for firms that already must address the general security risk issues associated with outsourcing to domestic sites. Madsen predicts a risk-rich future for MNCs and organizations that deal via electronic means externally beyond the borders of the United States. Security practitioners must account for these new types of security risks, and if applicable, they should have appropriate countermeasures deployed as part of the SRM program.

1.3 The Evolution of Information Security and Corporate Computing

The security of company business resources, including information, has been a historical, ongoing concern due to potential financial losses (Kendall & Scott, 1990; Perschke, 1986). The field of information security evolved from a focus on mainframe hardware, software, and procedures where the emphasis was on physical security and logical access

controls (White & Farrell, 1994). Mainframe computing emphasized efficient transaction processing and was usually depicted as a centralized operation where the governance (uses and users) of the technology was under the complete control of a central authority. The focus was on the control of information flow, and security measures were more likely reactive rather than proactive (Abrams & Moffett, 1995). The computer center was an island of technology secured by locked doors, with access exclusively granted to known personnel, and those off the island held little computer related technical knowledge. The physical and logical security (confidentiality, availability and integrity) of the IT resource was under the exclusive control of the central authority (Merten & Severance, 1981).

It was rare for any non-governmental/military organization to have a formal SRM program (Bates, 1970; Lindup, 1995). Because there were no user interface issues, there was no need to evaluate possible tradeoffs between ease-of-use and information security in formulating a security policy (Wood, 1995). If available at all, security policy might have been considered in a disaster recovery plan to protect the physical environment of the mainframe in order to maintain the data processing activities of the organization (Meade, 1993; Wessler, Myers, & Gardner, 1971).

The Foreign Corrupt Practices Act (FCPA) was enacted in 1977, and it was responsible for many firms to initially establish a computer security function (Tipton, 1994). The FCPA mandated that top management must implement internal controls relative to the business transactions and organization processes (Fisher, 1984). Possibly due to the passage of the FCPA, a survey conducted by Merten and Severance (1981) reported that 61.2% of 673 corporate executive respondents stated that electronic data processing was their greatest internal control concern.

Typical organizational structures were hierarchical in nature, and the focus was on coordination and control; IT was used as an implementation device for coordination and control (Venkatraman, 1994). The risk management function of organizations was primarily concerned

with catastrophic risks associated with natural disaster while other business risks were usually handled by corporate treasurers and legal counsels (Olsen, 1995).

The era of office automation applications used personal computers (PCs) to enhance the efficiency of individuals and functions (Paddock & Scamell, 1984; Raho & Belohlav, 1986). During this era the IT resource was still being used to support functional efficiency as a coordination and control mechanism (Cash et al., 1992; Daniels, 1991). The governance of the IT resource and the security responsibility might have been centralized or possibly shared between the central authority and the individual user group. Davies and Price (1984) warned that there probably never would be any systematic methods for dealing with information system security in this end user computing environment; special emphasis would have to be placed on system software and people-related security measures.

The results of a survey of IS and general executives during this period indicated that while they recognized the increasing importance of data as a corporate resource, security and control were still considered a technology and application issue and not a major corporate issue. In fact, security and control had slipped in importance from 12th to 18th between 1980–1986 (Brancheau & Wetherbe, 1987). On the other hand, surveys conducted with security specialists revealed their increased concerns about connecting PCs in functional areas with corporate mainframe computers. A survey conducted by Boockholdt (1989) revealed a growing concern about end users gaining access to mainframe resources. The participants in the survey indicated that intentional or unintentional security breaches would result due to end users downloading and uploading data and files from PCs into mainframe data files. Frank (1988) cited several examples of an increased level of concern being voiced by both the academic community and by practitioners over the governance and security requirements of this end user computing (EUC)/PC environment. The security and governance of the IT resource may still have been centralized or there may have been both shared responsibilities between the central authority and the individual user and functional group (Bergeron & Berube, 1990). There were reports

that the total security responsibility for both standalone PCs and EUC in general was being totally distributed to the individual user or functional groups (Frank, 1988; Tipton, 1994). There was growing evidence that many IT-related business disasters were associated with human activities. According to statistics compiled by Contingency Planning Research, at least 21.4% of the business disasters it tracked between 1980 and 1993 were caused intentionally and 12.8% were due to intentional or unintentional human errors (Meade, 1993).

During this era, The Trusted Computer System Evaluation Criteria (TCSEC) of 1985 was used by military/government IT users. The paradigm behind the TCSEC was to provide the minimal number of security breaches regardless of the costs associated with the countermeasures. The TCSEC was context-independent in the sense that particular processing environments were not considered, and no tradeoffs were allowed for system performance or potential applications (von Solms, Eloff & von Solms, 1990). However, the TCSEC could not be easily applied to business organizations that have to allocate limited resources to maximize overall organizational performance. The reported conclusion of a study conducted by the National Research Council (1991) sums up what many believed: "The state of computer security in the U.S. was in a mess" (Loch, Carr & Warkentin, 1992).

The present era has been called the 'era of open systems', and it is characterized by distributed IT resources and by levels of electronic integration (EI) beyond traditional organizational boundaries. The platform foundation consists of standard nonproprietary operating systems, user interfaces, application standards and network protocols.

There is widespread use of interorganizational systems (IOS), and electronic data/document interchange (EDI) (Benjamin, de Long & Scott Morton, 1990). Additionally, organizations are incorporating e-mail, wireless communications (Lathrop, 1992), portable computers, and imaging technology in their business processes (Fried, 1994). Finally, there is a reported explosive growth and widespread emergence of organizational Intranets, using

Internet technology, allowing employees to find organizational information wherever it resides (Anderson, 1997).

Today, for many business organizations, data and information have become a strategic resource which, if mismanaged, could lead to the immediate loss of a strategic advantage or to a catastrophic financial loss (Grant, 1992; Vitale, 1986). The security practitioners must understand the complexities of business processes that must be looked at in ways that require everyone to understand their stakeholder roles in the security of the IT resource (DeMaio, 1995; Poore, 1995). In many cases, distributed computing environments and increased electronic integration (EI) levels are being used in strategic alliances that require sharing firm knowledge bases (proprietary information). These strategic applications of IT carry with them potential business, security, and legal risks (Hoppe, 1994; Lightle & Sprohge, 1992; McGaughey, Snyder & Carr, 1994; Tipton, 1994; Vitale, 1986).

Strategic alliances have been forming at an accelerating rate over the past decade (Lorange & Roos, 1991; Ohmae, 1989). It has been reported that strategic alliances increased 47% annually in the 1980s (Work, 1988). These strategic alliances, which are a form of cooperative venture, can introduce security risk issues for the firm's IT resources that were not present when their existing security policy was formulated (Reich & Makin, 1986). Today, it has become apparent that SRM goals must become totally integrated with the overall strategy of business organizations during the strategy making process (SMP) (Olsen, 1995).

With the increasing use of the Internet by business organizations and the explosive growth of Intranets for enterprise-wide communication and computing that include customers, the risks associated with the security of the IT resource have never been higher (Anderson, 1997). The director of special projects for The National Computer Security Association (NCSA) highlighted a major security risk associated with connecting organizational information resources via the Internet:

Firewalls have been called condoms for corporate networks. They provide digital protection for participants in the packet-level intercourse associated with the rapid growth of Internet working and commercialization of the Internet. As with condoms, many people have heard of Firewalls, and some people use them. However, the number of security incidents arising from Internet connectivity strongly suggests that not enough people are using them properly. (Cobb, 1996)

Paradoxically, firms only using Intranets are not safer than firms using the Internet, since current estimates claim that as high as 80% of total security losses are due to company insiders (Violino, 1996b). Poore (1995) states it most straightforwardly, "Open network and security form an oxymoron when used together" (pp.22+).

Today the information security field must deal with security risk issues associated with open systems (DeMaio, 1995a; Reid, 1995), the full reach and range of the IT platform (Keen, 1991; Tan, 1995), the strategic exploitation of electronic integration (Venkatraman, 1994), the further implications of connectivity and networked organizations (Venkatraman, 1994), and the increased presence of competitive intelligence (CI) operatives (private firms and foreign governments) who strive to gain company proprietary information (Fine, 1995; Kailey & Jarratt, 1995; Madsen, 1995; Smith, 1995). Additionally, with IOS applications and outsourcing of IT development and data processing, many organizations now have to share security responsibilities with external agents (Madsen, 1995; White, 1991; Wood, 1995).

The advent of interorganizational systems (IOS) has the potential to penetrate the security shield protecting the technical [knowledge base] core of the firm (Thompson, 1967). The introduction of IOS in essence has created potential paths to the internal organizations systems and processes that are open to customers and suppliers (Doz & Prahalad, 1991; Fried, 1993; McGhie, 1994). In an internal report published in 1994, the Aerospace Computer Security Associates (ACSA) recognized the complexities faced by today's information security community. They recommended the introduction of a new paradigm that recognizes that security is a global property that must be addressed in this larger, more heterogeneous

environment (Abrams & Toth, 1994). This type of situation was correctly envisioned by Bates (1970), when he pinpointed the organizational vulnerabilities associated with “those systems which are communications oriented, since they are probably the systems of the future” (p. 61).

Today, the organizational structure may be traditional, matrix (Duncan, 1979; Burt & Celotto, 1992) or one of the emergent non-traditional forms (i.e., horizontal, virtual) (Byrne, 1993, 1993a), networked (Bovasso, 1992; Miles & Snow, 1995), or modular (Tully, 1993). Many of the emergent organization forms are more organic, loosely coupled, team-focused entities. The rapidly changing business environment is requiring organizations to redefine how they use knowledge throughout the value chain. It is a requirement that many of today’s and tomorrow’s business organizations must be able to freely communicate and to use knowledge (Daft & Lewin, 1993). The emergent organizational forms are more process focused than the traditional organizational forms and a dysfunctional situation may occur between the controls required for security and organizational control requirements (Herold, 1994). DeMaio (1995a) stresses that when these new organizational forms require a rapid movement to totally distribute and network resources, the security and governance of the technology may be under the management of people who lack the level of technology training required to manage the technology properly. Therefore, it becomes extremely important that management fully understand the downside risks associated with these situations.

1.4 Management Support for SRM Programs

In 1989 Rockart and Short reported that the top management of companies does not support the necessary measures to secure the firm’s IT resource. At the same time, there were surveys that revealed that the IS professional community may have been partially responsible for this situation. Kim and Kim (1999) conducted an in-depth evaluation of six MISQ surveys between 1980 and 1995 that shows that IS practitioners did not consider information security to be an important issue before 1995. In 1995, the issue was ranked fourth in importance versus

nineteenth in 1989. The lack of importance placed on information security by both the TMT of organizations and the IS practitioner community has resulted in serious business consequences for organizations. It is important that awareness of information security must be elevated in the organization and be viewed as any other TMT business issue.

The results of a survey, conducted by Information Week/Ernst & Young, revealed that nearly 50% of the 1,293 responding firms had lost information they considered valuable. Since 1993 at least 20 respondents stated they had lost information valued at more than \$1 million. Additionally, possibly due to dramatic growth in the reported business losses associated with security breaches, more than 75% of the respondents reported they have a full-time information security director (Panettieri, 1995). An earlier report of a survey conducted in 1993 by Information Week/Ernst & Young reported that 22% of 870 CIOs responding, reported that their organizations viewed security issues as fairly unimportant or extremely unimportant. The only two industries that reported security issues as extremely important were banking and stock brokerage (Panettieri, 1994). The results of the 1998 Information Week/Pricewaterhouse Coopers survey seems to support the earlier views of a large segment of the U.S. security practitioner community. The 1998 global survey results ranked lack of management support as the number two reason blocking effective security programs. However, it was ranked number one by U.S. respondents (Dalton, 1998). Executive management perceptions and attitudes relative to the business risks associated with security risk may partially perpetuate this condition (Lewin & Stephens, 1994).

1.5 Security Risk and Business Decisions

How security risk is managed is a business decision. The decision is no different from any other business decision relative to using company's resources (Hill & Smith, 1995). Today, business organizations should realize that they must view risk in a holistic framework that requires recognizing the "net risk" at all levels of the organization (Haines, 1991; Vojta, 1992).

The rapid adoption of advanced IT puts severe stresses on organizational enabling mechanisms that had known capabilities to handle various levels of vertical complexity, horizontal complexity and spatial complexity. The existing IT resources used to support these organizational enabling mechanisms are themselves coming under stress (Lightle & Sprohge, 1992). Furthermore, these same organizations are using advanced IT for applications internally and beyond the organizational boundaries (Daft & Lewin, 1993).

Today, management teams are incorporating IT in their business strategies. The TMTs are making these strategic decisions under varying levels of uncertainty that are potentially increasing the level of security risk associated with their IT resource. How these firms formulate and implement their SRM programs will depend to a large degree on how their management view the perceived potential harm and benefits associated with the deployment of the IT resource. The IT security risk issues and the related business and strategic risks associated with their current IT resource posture have to be considered. Therefore, the risks associated with the security of the information resource are strategic risks (Kendall & Scott, 1990; McGaughey et al., 1994). As with all risk related issues, there are multiple tradeoffs, priority concerns and multiple consequences that should be addressed during the decision making process (Barton & Gordon, 1987). For business organizations security must not be treated as a technology issue; it is an important strategic issue (Highland, 1992). Yet, general management may still be offered simple guidelines to deal with the complex issues associated with the security of the IT resource in the distributed and open environment (Regan & O'Conner, 1994).

1.5.1 Information Security Management

The scope of Information Security Management (ISM) includes policy, risk analysis, risk management, contingency planning and disaster recovery (Forcht, 1994). Frameworks have been suggested that view these dimensions within different environmental contexts in

order to develop a general model of ISM (von Solms, van de Haar, von Solms & Caelli, 1994). There are some sources that suggest ISM should be viewed as any other organizational issue that requires individual management intervention (Fagan, 1993, Wood, 1991). Therefore, in order to establish an information management strategy, the overall organizational business strategy and its coordination and control requirements must be evaluated relative to a family of risk continuum. The development of cost effective security measures that support organizational goals can only be implemented through higher levels of management participation and involvement (Blackhouse & Dhillon, 1995). Management must selectively align the organization risk management posture with the business goals of the organization (von Solms et al., 1990).

1.5.2 Emerging SRM Issues

Organizations today face an uphill battle as they learn to manage the complexities of the components of the integrated IT platform and simultaneously cope with the operational issues associated with integrating the overall IT platform with the business strategy of the firm, the overall goals and objectives of the organization, the governance system of the organization, and the overall corporate strategy of the organization. The required SRM program decision-making process is being conducted under less than certain conditions.

Within the context of the hierarchical mainframe security model, risks were associated with the level and duration of a discontinuity in the service level of the supporting computing resources available to the organization. Hence, security was a matter related to the integrity of computing systems rather than data, information or systems (Loch, Carr & Warkentin, 1992).

Today the risk management strategy must be integrated with the overall corporate strategy (Froot, Scharfstein & Stein, 1994). The emphasis of information security policy should shift from risk prevention to risk management and organizations must include security risk considerations in the SMP of the organization if they want an effective program.

1.6 Recommendations for Change

Security specialists seem to be confident that they can manage the security risks associated with introducing the latest IT into business organizations (Hamilton, 1995). They also tend to agree that they have the proper technology available for reducing the security risks associated with advanced IT usage (Cassidy, 1994). However, there is growing consensus that advanced IT systems are becoming unmanageable and that new tools and advanced levels of training are required for the personnel who operate them (Wood, 1995b).

Today, there is recognition that user awareness is crucial and that technical controls and administrative procedures must be linked with user cooperation and user acknowledgment of their roles in providing security for the organizational information resource (e.g., Highland, 1992; Kay, 1994; Mork, 1996). Additionally, the ultimate responsibility for information security rests on the shoulders of top management (Price, Cotner & Dickson, 1989; Thompson, 1995). Today, top management must take an active support role in SRM programs. The level and composition of their active support should be identified and monitored since it may be a major contributing factor in the overall effectiveness of the SRM program (Jarvenpaa & Ives, 1991). Finally, that security policy issues must be addressed within the context of the overall strategic decision making process. The business organization must include security issues (threats, vulnerabilities and the cost-effectiveness of potential countermeasures) as part of an overall strategic plan (Hoppe, 1994; Stahl, 1993).

1.6.1 Emergent Security Paradigms

The combination of rapid changes in IT (types & application) and the task environmental demands that are incubating new organizational forms will require a reengineering of security administration (White & Farrell, 1994). Today's environment entails dealing with the vagueness and imprecision of humanistic systems. Security itself must be treated as a dynamic environment where the threats may change rapidly and dramatically

(DeMaio, 1995). What is recommended is a security paradigm shift away from a focus on a goal of absolute security to one of relative security.

Blackhouse and Dhillon (1995) have suggested that the focus must be on the patterns of behavior associated with the overall security of data in organizations. They recommend looking at the “information environment” of an organization using semantic schema so researchers can represent underlying structures in a cultural context. Additionally, security measures should focus on prevention; these measures can only be achieved through coordinated actions at the firm level and the social level of organizations. Hitchings (1995) advocates that the new paradigm should be based on human issues similar to those considered by Checkland (1981) and by Checkland & Scholes (1990) in their soft systems methodology. This methodology presents a holistic approach in that it captures the entire stakeholder community and incorporates their various perspectives. Baskerville (1992) identified a fundamental generation gap between the developmental process of information systems and the development of their security. Baskerville contends that the logical engineering methods of third generation systems development are in a permanent state of tension with the mechanistic approaches to security design. Additionally, to be successful there must be an emphasis on behavioral aspects of information security that include motivation, cognition and the role of the system in the organization. The next generation of systems development must include a methodology that develops the information system and its security requirements together. There are others that simply suggest that organizations must have a security strategy backed by a strong formal security policy that focuses on all aspects of the IT resource (Wood, 1995). Finally, some contend that a new paradigm is not required. They contend that the major problem is a general managerial confusion caused by a lack of an international regime of information security standards. The standards could be used to develop the Information Security Management Model (ISM²) that could then be used to integrate the various dimensions of Information Security Management (von Solms et al., 1994). A similar back to basics position has been put

forth by Lichtenstein (1996), which contends that there does not exist a single set of security principles to draw on. Therefore, the security practitioner community is left to pick and/or choose from a wide and inconsistent set of principles. The author proposes an integrated Holistic Information Security model that is based on an extensive review of existing principles that have been integrated into a single set.

1.6.2 Suggested Risk Approach

Security risks occur at the strategic level, the operational level and the financial level. Therefore, these risks should be able to be incorporated in a globalized organizational risk management framework. Some general risk practitioner journals are calling for a new “holistic risk management approach” that will incorporate risk experts from all facets of the business in order to analyze all corporate risks to develop a global perspective towards risk (Barnham, 1995; Hill & Smith, 1995). Therefore, the risks associated with the IT resource should become a part of the overall risk aggregation of the business firm (Settembrind, 1994). The major focus of security practitioners will have to shift from functional security risk prevention issues to a paradigm shift that includes an organizational risk management methodology that includes risk awareness programs for all organizational stakeholders. Currently, many security practitioners only view the risks associated with the technology of security (Warman, 1993).

1.7 The Research Problem

No theoretically based research frameworks and models exist that are suitable to conduct research that addresses firm level SRM policy formulation content or process issues. Additionally, there are no constructs or valid, reliable research instruments to conduct this type of research at the firm level. Straub (1989) reminds IS researchers that rigorous procedures are required to develop valid, reliable research instruments to empirically measure adequately developed constructs. The extensive IS and security literature streams reviewed for the proposed research study lacked theoretically based empirical research studies specifically

focused at the firm level issues the IS security function must address. The majority of the literature is based on opinion, anecdotal evidence, or solely practitioner experience. There are descriptive surveys, case studies and research studies related to specific aspects of the issue. However, no empirical studies were found that address the multifaceted nature of firm level SRM issues. The results of such research studies could aid management during their security policy decision-making process and prove useful for the security practitioner community in developing and administering effective SRM programs. The research should incorporate other disciplines in order to aid the professional risk takers responsible for these decisions (MacCrimmon & Wehrubg, 1990). These managers are being asked to address the potential business risks associated with the increased threats to their organizational knowledge base due to the vulnerabilities associated with open systems and distributed architectures, while at the same time, they are being asked to provide increased levels of open systems required by current business realities (Kruys, 1991). Senior management is not being made aware of the potential personal legal risks they face if they do not use available information to “prudently” protect the company stakeholders by applying the information to “prudently” protect the company IT resource (Fried, 1994). Recently, there has been renewed emphasis that management must take an active role in both assessing the effectiveness of security policy and communicating the importance of security awareness to all interested stakeholders (Warman, 1993). There are companies that are instituting major security awareness programs that encompass the entire organizational stakeholder constituency and emphasize that security is everyone’s responsibility (Herold, 1994). The top management of these organizations may have recognized that a sound, cost effective SRM program is a necessary cost of doing business in today’s environment (Christine, 1995).

1.7.1 Research Goals and Objectives

The overall goal of the research study was to conduct a firm level empirical study investigating effective and ineffective SRM programs. The immediate objective of the research study was to empirically test the relative importance that executive management support, the actual performance of the SRM program, and the gap between the desired performance and actual performance have on the perceived effectiveness of the SRM program. The second objective was to develop an SRM program construct that could be used to conduct organizational level SRM research and to empirically test some popular anecdotal and practitioner reported conflicting suggestions and recommendations in establishing the desired performance level expected from the security risk management program.

1.7.2 The Research Approach

The research approach incorporates two basic premises: (1) “The study of (the impact) IT and IT management in isolation from their environment could yield highly misleading and constricted theories” (Baskerville & Smithson, 1995, p. 69); (2) That “above a certain baseline level of common security needs for similar threats, vulnerabilities, and types of information systems, each type of organization with a different mission has different security needs as well” (Parker, 1995b, p. 3+). These premises guided the literature review for the research study.

The review of the relevant literature suggests that a major determinant of the effectiveness of SRM programs is the actions of top management relative to the security strategy formulation process. The perception management has about the types and levels of business and security risks present in the task environment shape the organization’s responses to risk. These perceptions directly influence what the organization will expect from the SRM program. Additionally, the literature has suggested that the actual performance of SRM programs has a major impact on perceptions held by organizational management about the effectiveness of existing security measures. Finally, management knowledge about potential

security risks and their risk propensity and trust attitudes have a direct influence on the desired performance expected from the SRM program.

The marketing literature suggests that the gap that exists between the desired performance and the actual performance of a product or service directly influences the perceived effectiveness of a product or service. This disconfirmation/confirmation concept has been adapted in a recent EUC satisfaction study (Suh, Kim, & Lee, 1994) and a conceptual model has been suggested based on the same disconfirmation/confirmation paradigm. The conceptual model has been suggested as a suitable vehicle for conducting research studies that extends the user information satisfaction knowledge base (Shirani, Aiken & Reithel, 1994). A conceptual research model that integrates these models and adds the reported importance of executive management support for program success was used for the dissertation research study.

The proposed research study was planned to test the relative importance of the IT resource posture and firm management characteristics in determining the desired performance demanded from an organizational SRM program. When we research the decision making process, we must be aware of the importance of the individuals within the group responsible for the decisions (Chakravarthy & Doz, 1992). Additional testing was to include the relative importance of the actual performance of the SRM program and the relative importance of executive management support in determining the overall perceived effectiveness of the SRM program. The importance of executive management support (involvement and participation) in the progressive use of IT in the firm has been identified as a major contributing system success factor (Jarvenpaa & Ives, 1991). The focus of the research study will not be on technical factors but rather on the organizational, social and political factors that some IS research has called attention to (Johnston & Vitale, 1988; Scott Morton, 1991; Willcocks, 1992).

1.7.3 The Importance of the Research Study

The research study was to contribute to the knowledge base in the IS field by investigating how the effectiveness of SRM programs can be improved through direct intervention by security practitioners. The study was to accomplish this by exploring selected important relationships that may be influenced by direct intervention. These include:

1. The relationship between the SRM Program and the Actual Performance of the SRM Program
2. The relationship between the IT Resource Posture and the Desired Performance of the SRM Program
3. The relationship between Firm Management Characteristics and the Desired Performance of the SRM Program
4. The relationship between Executive Management Support and the Effectiveness of the SRM Program
5. The relationship between the Actual Performance of the SRM Program and the Effectiveness of the SRM Program

The research study is original in the sense that the literature review did not uncover any studies that have empirically investigated the antecedents of effective SRM programs. Additionally, the development of measures for the effectiveness of SRM programs should prove beneficial for security practitioners and managers in order to gauge what is required to successfully compete for the resources required to improve SRM program effectiveness.

1.8 Limitations of the Research

The research study focused on business organizations located in the United States. Therefore, the results cannot be generalized to the public sector or to firms outside of the United States. The research study was to include a tightly integrated strategy of in-depth interviews and other data collection methods with the management at two firms located in a

northeastern metropolitan area followed by survey research (Krammer & Dutton, 1991). This cross sectional approach severely limits attempts to identify the cause-effect relationship between the variables included in the research study. The research population consisted of organizations throughout the United States. The initial sample of organizations came from a heterogeneous population based on organizational contextual variables that included: sales, number of employee, industry sector. This action limited any attempt to associate the results in terms of applicability to any single industry or organization. The aim was to strive for the maximum level of industry generalizability as practical. A restriction on the generalizability of the results could have occurred if steps were not taken to check for nonresponse bias. When there are statistical differences between those firms that respond and those that do not respond the research results cannot be safely extended to the target population. This would severely limit the generalizability of the study. The sample of firms was selected from a population of organizations that was expected to have an established security culture. A potential problem with this approach is that many of the firms that respond may not have a SRM Program in place for a sufficient length of time. This effectively reduces the power of the statistical tests due to limited sample size. The population sample was to be drawn from the membership listings of selected ACM Special Interest Groups (SIGs). The firms in the population were to be screened for diversification. The organizations that generate a significant portion of their firm sales in more than one primary industry would have been eliminated. This action was to be taken to avoid the problem of multiple task/multibusiness organizations. This step was to be used to further insure that management had focused on the primary firm level risks that have helped to shape the existing SRM Program, business strategy, structure, controls, and IT resource posture. Again, if most of the firms that respond generate a significant portion of their sales in more than one primary area, excluding these firms would limit the power of the statistical tests due to limited sample size.

1.9 Organization of the Remainder of the Dissertation

The remainder of the dissertation contains five additional chapters.

Chapter 2, Literature Review, Research Model, and Hypotheses: Chapter 2 contains the theoretical and empirical foundations for the research model, the rationale used to establish the domain of the research model, and the development of the dissertation hypotheses. Additionally, it contains a review and evaluation of relevant risk and IS security research conducted to date.

Chapter 3, Research Strategy and Methodology: Chapter 3 contains the process used to formalize the specific research domain. Included is the operationalization of the constructs, the rationale used for the development of the research instruments, the statistical methodology that was used to analyze the data after it was collected; the methodological issues that guided the tradeoffs related to the selection of the final method of investigation, and the choice of data collection methods. Additionally, chapter 3 contains a description of the methodology that was to be used for testing instrument validity and reliability, sample selection, and the general statistical method that were to be used to test hypotheses.

Chapter 4, Revised Research Strategy and Response Rates: Chapter 4 is divided into major sections that include the pilot test results, the resulting major research strategy changes that were required after the pilot test, and the response rates obtained from the mail survey.

Chapter 5, Interpretation: Chapter 5 is divided into major sections that include the firm level results that were obtained, individual descriptive statistics, and an evaluation of selected firm level results.

Chapter 6, Contributions and Recommendations: Chapter 6 is divided into major sections that include the contributions of the study, the limitations of the research study, the lessons learned and recommendations to guide future research in this area.

CHAPTER II
LITERATURE REVIEW, CONCEPTUAL RESEARCH
MODEL AND RESEARCH HYPOTHESES

2.0 Introduction

The chapter contains the rationale used to establish the domain of the research study and the basis for the relationships that are in the conceptual research model. Additionally, the chapter contains descriptions and evaluations of relevant risk research and a summary of selected IS related security research. The major literature streams used to develop the hypotheses that were to be tested with the modified research model are cited by appropriate section.

2.1. Definitions of Risk

To conduct research about SRM programs one should have a commonly held definition of risk. Risk, as a concept seems to have many elusive properties. Starting with several definitions in a popularly used dictionary, we could start with the following:

risk (risk), n. **1.** Hazard; peril; exposure to loss or injury. **2. Insurance.** **a** The chance of loss or the perils to the subject matter of insurance covered by the contract; also, the degree of probability of such loss. **b** Short for amount at risk, that is, the amount which the company may lose. **c** Loosely, a person or thing considered with reference to the risk involved in placing insurance upon him or it. **d** The character of hazard involved in insurance; usually with a qualifying word; as war risk, fire risk, catastrophe risk. (Webster's New Collegiate Dictionary, 1957, 731-732)

A commonly held definition of risk used in engineering and project management is "a function of the probability of an undesirable event and by the severity of the consequences of that event"(Shtub, Bard & Globerson, 1994, p. 260). In the business world, a commonly held definition of what risk is "the uncertainty of financial loss, the variations between actual and

expected results, the probability that a loss has occurred or will occur” (Hill & Smith, 1995, p. 201).

The three purest definitions found were: (1) risk, in its most basic form, is the uncertainty associated with any outcome (McKim, 1992, p. 7), (2) a risk is any unintended or unexpected outcome of a decision or course of action (Wharton, 1992, p. 5), and (3) risk is the perceived extent of possible loss (Dean, 1996). Dean contends that with the growth in the knowledge base of fuzzy logic and fuzzy systems, the general concept of possibility seems to be more closely related to thought and perceptions than probability. Dean further contends that since individuals make business decisions for organizations their perceptions of risk as members of organizations are the basis of firm level risk management. Their goal is to maximize possible gain, minimizing possible loss. This parallels the notion put forth by Bodeau (1992) in the development of the conceptual model of disclosure risk for information systems. In the development of the conceptual model for the Analysis of Networked Systems Security Risks (ANSSR) prototype, the term “likelihood” is used rather than probability in how the term “risk” is used. The reason given is that in most cases there is a lack of useful statistical data for evaluating the probability of a loss and for assessing the magnitude of the loss (Bodeau, 1992).

For the dissertation the concept of risk with a focus on the downside aspects proposed by Dean (1996) was used. The concept is ideally suited for investigating the role that risk plays for the management of organizations responsible for the tradeoffs that have contributed in shaping the current SRM program. Additionally, recent empirical research suggests that the downside nature of risk is a major factor in determining risky decision making behavior by firm executives (Sitkin & Weingart, 1995). Finally, managers involved in the same decision making process view the magnitude of the risks differently (Kahneman & Tversky, 1982).

2.2 Classical Risk Management

The classical decision theory school is founded on the assumption of expected value as the sole basis for the decision making process. The rational school of risk management

contends that subjective factors must also be considered in managing risk. The issue becomes more complex at the organizational level since the TMT may not be able to view risk with either perspective (March & Shapira, 1987). Slovic et al. (1977a) found that individuals do not prefer to insure against low probability disaster. In fact, they prefer to insure against smaller losses, which are more likely to occur. Lichtenstein et al. (1978) found that people tend to underestimate the probability of events that are relatively undramatic and frequent. They also overestimate the probability of events that are dramatic, infrequent or have not happened for a long interval of time since the last occurrence. In information security risk management both schools appear to have a strong position in terms of the methodologies being utilized in the risk analysis phase of the risk management cycle.

2.2.1. Risk Management Techniques

Classical Risk Management handling techniques generally fall into two categories: simple risk adjustment (SRA) and probabilistic risk assessment (PRA). Either of these techniques are generally used by business firms when they are required to make capital investment decisions (Ho, 1992). Regardless of what technique is used, there are several research streams that emphasize the importance of multiattribute utility theory (MAUT) when studying decision making behavior under uncertainty (e.g., Farmer, 1993; Stephanou, 1987). MAUT has been used widely for analyzing sets of alternatives that had multiple objectives (e.g., Merkhofer & Keeney, 1987). In a pioneering work on multiple criteria decision making Keeney & Raiffa (1976) suggest several uses of MAUT. These types of analysis are all associated with classical decision theory that requires the use of expected value (EV) as the only criteria for evaluating the decision alternatives (McKim, 1992). Therefore, the use of classical decision theory will not be utilized for the proposed research study.

2.2.2 Risk Analysis and Risk Assessment

The general purpose of risk analysis has been to isolate and identify possible outcomes of decisions while risk assessment has been focused on the estimates of the probabilities and the relative level of the outcomes. Risk analysis and risk assessment, both quantitative and qualitative, have been major tools in developing an estimate of loss expectations associated with specific types of threats. The field has evolved from two perspectives that have dominated. First, the insurance industry approach is concerned with a company's exposure to physical loss in order to arrive at annual insurance premiums (Stahl, 1993). The second approach has evolved from the audit domain of accountancy. This approach uses a checklist methodology to determine the conformity or nonconformity against a set of universally accepted standards. The second approach has been successfully adopted by EDP auditors to evaluate company efforts relative to virus prevention and detection efforts in microcomputer based environments (Joseph, 1990). A third methodology is based on a heuristic approach. The approach uses a series of scenarios and then uses estimated probabilities of occurrence to evaluate risk levels (Sommer, 1994). In general, the field of risk analysis has been dominated by these perspectives (e.g., Baskerville, 1988; von Solms et al., 1994; Enger & Howerton, 1980; Fisher, 1984; Hamilton, 1973). Today, regardless of what level of "sophistication" is used throughout the risk management process, the end result must be a systematic approach which is a cost-effective, non-technology driven, value creation process which contributes to the overall effectiveness of the organization (Hill & Smith, 1995; Troy, 1995). However, there should be a cautionary note assigned to using annualized figures when assessing risks associated with a catastrophic security event. "There is no realistic way to spread the costs and economic losses associated with a disaster over time" (Menkus, 1992, p. 213).

In reviewing the literature on information security risk management, there appears to be a problem due to getting a clear understanding of what "risk analysis" is. Reviewing several automated risk analysis methods, Eloff et al (1993) found a considerable lack of consistency in

the terminology being used. A major finding was that the term “risk analysis” was used to identify objects needing protection and in some cases “risk analysis” was used to describe other risk management activities.

The adoption of the risk management perspective does not drive the level of security risk to zero. “In every human action or decision the question is never one of whether or not to take a risk but rather which risk to choose” (Wharton, 1992, p 3). Simply, considering risk assessment via assets and threats is a necessary but not sufficient condition. Since risk management is decision making under uncertainty, it may be that existing techniques used for current risk management approaches are not applicable to managing the risks associated with security (Abrams & Toth, 1994).

2.3 SRM Program Scope

Historically, threats and vulnerabilities were considered after they had caused security breaches. The concept of applying risk management techniques based on a continuous cycle of risk identification, analysis, assessment, resolution and monitoring that should proceed continuously before an actual occurrence of a security breach is relatively new and is due primarily to the increased size, complexity, and dependency of organizations on advanced IT applications. Furthermore, human issues must become a main focus item since people are the main contributing factor for all information security breaches (Hitchings, 1995). The increased importance and potential business risks associated with the disclosure, modification, unavailability or destruction of information intensifies the potential business impact of a security breach.

Arriving at acceptable solutions related to these issues will require a dramatic paradigm shift from the pure military paradigm that is based on a Mainframe based-platform using hierarchically structured security levels and a centralized authority to a new paradigm that includes networked peer relationships that must include trust relationships required for the high levels of connectivity required by the new information technologies (Rangan, 1992).

Furthermore, since most existing security models do not include the concept of non-hierarchical relationships, they would not be appropriate for organizations employing levels of Electronic Integration (EI) that may include interorganizational systems, global networks and electronic knowledge integration (cf. Bovass, 1992; Jarvenpaa & Ives, 1994; Rockart & Short, 1991). These organizational configurations will be using combinations of business and IT governance that will require a proactive risk management approach (soft posture) rather than the traditional risk prevention approaches to develop appropriate security risk management programs that are capable of generating counter measures that adequately address the accompanying levels of security risk. The accompanying business risks will also have to be simultaneously evaluated and analyzed. Sherer (1995), contends that security will be the major firm level technical issue as more companies adopt IOS that include the exchange of proprietary information. Additionally, the author suggests that if “security risk is not adequately reduced, this role (the trust intermediary to reduce competitive risk) may continue once these systems are developed”. Finally, in the task environment people are the competitors, customers, suppliers and leaders of the other firms. Ultimately, security is a people issue since these people are the stakeholder/consumers that must be satisfied with the effectiveness of the SRM program.

2.3.1 Threat Classification

There have been many different classification schemes developed grouping threats by major categories (e.g., Rainer, Snyder & Carr, 1991). Regardless of how many threat classification schemes are developed for whatever reasons the author intended, the intentional and unintentional threats to data can be resorted into general categories developed by Parker, (1995c). Additionally, Parker (1995) expanded an existing category by adding Possession to Confidentiality and he established exposure to threats as a new category (Parker, 1995c). These modifications were suggested due to the additional information security issues that must be addressed in distributed and open systems environments (see table 1). For the purposes of this

dissertation, “threats” will be classified using the Parker categorization. Threats to the IT resource of an organization emanate from natural, unintentional or intentional sources and are directed at one or more of its vulnerabilities (Bennett & Kailey, 1992).

2.3.2 Vulnerability Classification

For the purposes of this dissertation, ‘vulnerabilities’ are classified using the Regan & O’Connor (1994) scheme. The vulnerability of an organization’s information resource can be identified and classified as one of the following: Physical Security, Natural Hazards, Hardware and Software Faults, Media Damage or Destruction, Electromagnetic Signal Emissions, Telecommunication Comprise, and Human Beings. There is general agreement on these categories, and this scheme includes specific IT resource vulnerabilities present in the current distributed and open systems environment.

2.4 Security Related Research Studies and Surveys

In reviewing the literature published after 1988, no substantial research studies were found that specifically address security policy formulation (content and process) issues at the corporate or business unit level. The studies that have been located address limited aspects of the security policy domain. The conclusion reached was the same one that Byrd, Sambamurthy & Zmud (1995) discovered in their review of IT planning literature. “. . . current IT planning research offers little guidance on the types of planning actions and behaviors (process issues) that are appropriate to organizational contexts. . . . limited empirical research has addressed this issue. Normative and perspective essays addressing the nature of the process . . . the content of IT plans, while relatively ignoring appropriate actions and behaviors associated with the IT planning process” (pp. 49-50).

The empirical research studies that were found did not address security related issues at the firm level of analysis. Furthermore, many were limited in scope due to a concentrated focus on one aspect of information security, some had methodological problems, or were limited to a

specific technology being utilized. Many of the studies that were found did investigate security concerns that include vulnerabilities and threats beyond the possibility of a discontinuity in the service level of the supporting computer resource. Finally, none of the research studies found addressed security risk utilizing the multidimensionality concept of risk. The following represent the scope of the limited body of IS/security research that was available to aid the development of the research study.

A study was found that empirically assessed cross-cultural differences in perceptions of the security risks associated with computer viruses. The study by Jones, Arnett, Tang & Chen, (1993) investigated cultural differences between Taiwanese (429 undergraduate and graduate) and U.S. (213 undergraduate and graduate) students, using three categories of perceptions. The three categories used were: (1) perceptions of personal susceptibility to viruses, (2) general perceptions of viruses, and (3) perceptions of viruses in their workplace. The authors contend that the results of their survey provides measures of general perceptions and awareness levels of viruses as well as beliefs about personal susceptibility and about the effect of viruses on the workplace. This study is at the individual level of analysis and did not prove suitable for developing the research methodology required for a firm level research study. Furthermore, it specifically focused on a single threat and therefore the reported results would not prove beneficial for supporting the theoretical foundations for the dissertation study.

The study conducted by Loch, Carr & Warkentin, (1992) investigated what the concerns of MIS executive were relative to the potential security risks associated with the vulnerabilities of a networked environment and also what the threats might include. The study included twelve threats that were extracted from the literature. The research focus was primarily the threat of computer viruses and preventative measures used to cope with the risks associated with this threat. A major reported conclusion was that managers' overall levels of concern for security may underestimate the potential levels of risk. This study while providing some interest again was limited in scope and therefore the conclusions provided proved to be of limited benefit for

the proposed research study. However, the conclusion relative to managers underestimating potential levels of risk may prove useful when evaluating the responses of the TMT concerns about security.

A survey by Bergeron & Berube, (1990) focused on organizational PC policies and end user satisfaction. The survey included responses from thirty-one organizations (thirty-one department heads and 211 microcomputer end users). Only one company did not have some type of PC management policies. The policies could be grouped into governance (purchasing, development, and support) and security, and 68% of the organizations had formalized organizational security policies. The authors concluded, based on end user responses as to what policies they respected, that in general an increase in the number of policies is directly related to reduced levels of end user satisfaction. Furthermore, they recommended that end user stakeholders should take an active role in policy formulation. The results of this study were supportive of many of the perspective suggestions found in the practitioner articles reviewed for the dissertation research study. However, the study did not include any information about the organizations that were included in the survey.

Another study by Frank (1988) focused on EU/PC quality control behaviors. The study used in-depth interview with 135 PC users from twelve organizations. The interview instrument included perceptual measures of specific departmental level security policies and the related activities required by the EU to be in compliance with them. The instrument included both self report and peer report measures. One of the conclusions reached by the author is directly related to security policy process issues. Namely, there may be a direct association between individual perceptions of departmental security norms (peer pressure) and EU security (file backup) behavior, and there may be no association between an EU perception of departmental PC security (file backup) policy and security (file backup) behavior.

Price, Cotner and Dickson, (1989) surveyed bank managers to determine their perceptions of the risks associated with potential computer fraud. The study focused on “what”

rather than possibly “why.” They reported on the 127 usable mail self-report questionnaire responses received back from 536 sent out to all of the commercial banks in Oklahoma. They reported that 86.9% of the bank managers perceived that a single breach in security could be costly to their bank; only 5.9% of the respondents perceived there was a high likelihood of their bank having a security breach. Interestingly 83% perceived loss of credibility as the major risk associated with a security breach. Only 48% of the bank managers reported their existing security policy included employee security awareness education. The authors concluded that commercial bank managers in Oklahoma had a high awareness of the sources (threats) to bank (computer files) systems and that they were aware of the most vulnerable types of computer files that might suffer a security breach. The results of this survey reinforce the inclusion of SR knowledge and awareness as dimensions of management characteristics in the theoretical model.

A research study conducted with academic institutions by Barnes & Harris (1990) investigated the general security of microcomputers physical protection, access control and software protection. The study focused on U.S. AACSB accredited business schools. The Deans at 192 of the 312 contacted responded with the names of the individual responsible for the governance of microcomputer facilities within school of business. Follow-up letters were sent out to the 192 individuals that were identified. There were 150 returned and the authors did not reveal the actual number of usable responses analyzed. The authors looked for consensus on security procedures being used. No questions were included about security policy. The authors recommend a college-wide security policy that is publicized to all faculty and students. However, there is no mention of any questions about security policy being included nor were they mentioned as a part of the reported survey results. They also make further recommendations and suggestions without any references to sources or how effective they have proven to be without any mention of tradeoffs in system performance, ease of use, complexity, and management time. They make further claims without any backup about universities being

lax in security procedures due to lack of experience. The reported results included : Hardware protection: 60.4% lab monitor assigned during working hours, security patrols when labs shut down; 40.9%, combination of deadbolt locks, intruder alarms, locking equipment to tables, windowless rooms. Combinations mostly used, no figures reported. Access control: 49% student I.D. checked for admittance, 16.8% had no controls on access. Software security: use manufacturers "key" diskette 32.9%, hidden files 20.8%, 65.1% students not allowed to remove software from lab. Prevent damage to software and databases: 71.8% write-protect labels, systematic backup of system 40.9%. Virus protection same procedures used as software protection, no percentages reported. The results of this survey were extremely limited in scope and did not prove to be of benefit for the proposed research study.

Goodhue and Straub (1991) developed a theoretical model of individual IS user security concern in order to investigate user perceptions relative to system security (see figure 1). The authors tested various propositions relative to the model specifically focused on individual levels of organizational concern for computer and data security. Their main objectives were to validate their theoretical descriptive model of the determinants of individual perceptions about the adequacy of the security of data and information systems. The overall purpose of the study was an attempt to understand what leads to higher levels of security concern among individual users of systems. The authors suggested that the validation of the theoretical model could lead to its use as a vehicle for developing programs to raise the security awareness levels in the general business community.

The model constructs are based on earlier research by Goodhue on individual user satisfaction . The three concepts that Goodhue used in developing a model of user's assessments of the satisfactoriness of a systems environment are used in the Goodhue and Straub model, (i.e., the task characteristics, the characteristics of the IS environment and individual specific characteristics) (Goodhue & Straub, 1991). However, for this study the authors defined these concepts and constructs within the context of providing organizational

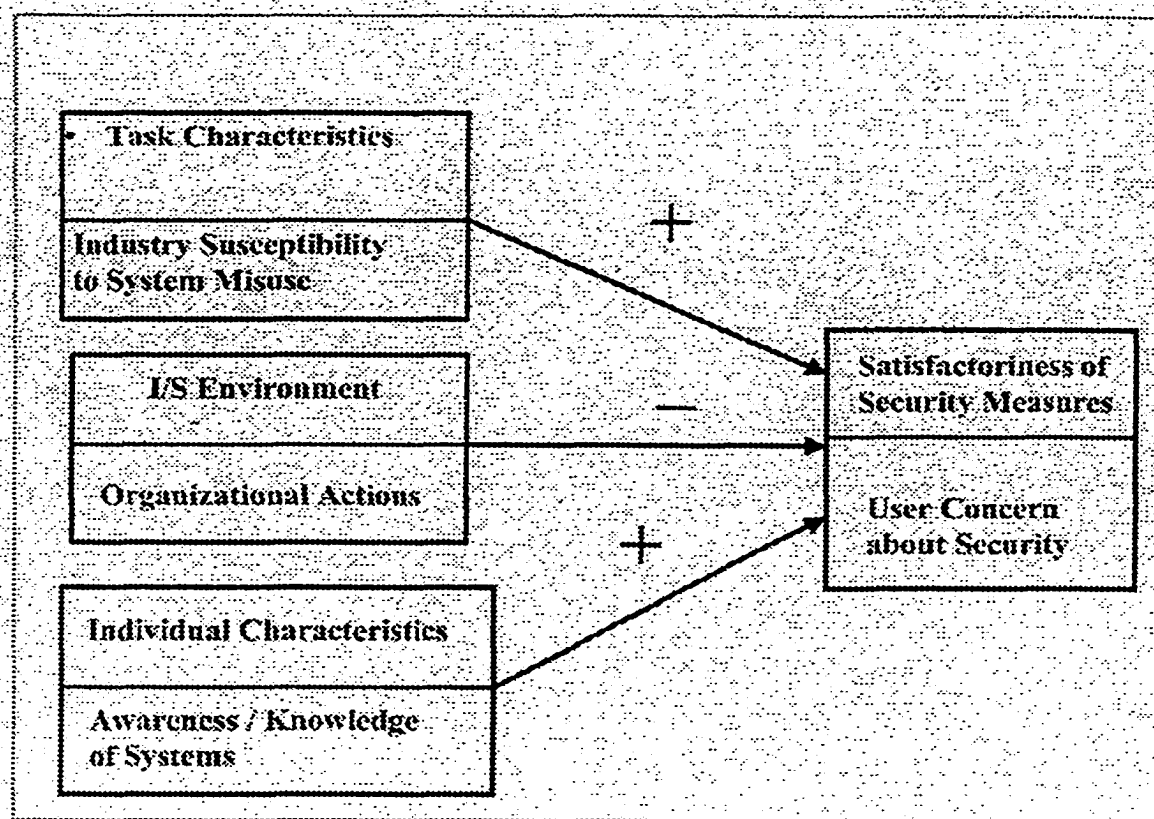


Figure 1. Theoretical Model of Security Concerns.

data and systems security. The authors tested four hypotheses using the theoretical model. The authors utilized a database that contained data collected from a victimization questionnaire administered to a sample of 570 randomly selected DPMA members that included 91% IS professionals. The questionnaire was originally used for a study of computer abuse and deterrent countermeasures. The constructs used are not the same as the ones used in the theoretical model. The authors also used the data from a questionnaire administered to 357 end-users at 10 organizations. The questionnaire was developed for a study of user assessments of the satisfactoriness of their environments. The questionnaire did contain measures of user concern about security and awareness/knowledge of systems. The authors reported that the factor analysis of the individual characteristic questions showed weak support for both reliability and discriminate validity of those measures. The

reported empirical results did not support the theoretical model. The authors admitted that using a *post hoc* analysis on data that was gathered from subjects from a prior study might not have been appropriate for testing the theory. The design of the original questions and the measurement validation process was conducted on constructs that were not the major constructs in the current research (Goodhue & Straub, 1991).

A survey of DP and MIS managers relative to use of PCs in the corporate environment was conducted by Raho and Belohlav (1986). The study is dated. However, it proved useful in the sense that it was conducted during the era of the proliferation of standalone PCs on the corporate scene. The survey involved 2,000 members of the DPMA, 452 usable questionnaires were returned and analyzed. Only 13.4% of respondents were holders of job titles outside traditional MIS functions. There was no indication that any of the respondents were involved in a security role within the firm. The survey contained a section relative to system integrity and security. However, the structure of the questions could not be usefully evaluated for the dissertation research study. The questions focused on how and which PCs should be used rather than specific security concerns.

A survey of DP managers was conducted by Merten and Severance (1981). The study is based on the results of a broader study, which included self report responses from 673 chief financial officers and in-depth follow-up interviews with 350 corporate executives in 50 of the firms that responded. While the study is dated, some of the findings have been instrumental in the conceptual model developed for the proposed research study. The useful findings were the following: company executives in general perceived that the present internal control systems were sufficient (risk/cost balance); company executives had limited knowledge of what controls were used by other firms in their industry. In general, company executives (415 of 673) were "worried" about what types of internal controls would be required, due to their companies' increased dependency on computers for operational effectiveness and financial reporting. The follow-up structured interviews were conducted with the chief internal auditor

and with the chief EDP official. Again, some of the results of these structured interviews proved beneficial for the proposed research study. The relevant ones are the following: responses from 20 of 54 EDP executives indicated that their most significant internal control concerns were about the loss of computer usage or security related (physical, data access or systems access); responses from 19 of the 54 EDP executives indicated that their most significant concerns were that existing control standards and procedures would not be adequate for the current environment; Only 3 of the 54 EDP executives held concerns that a trusted employee could do great harm to the operation.

Lim and Jamieson (1995) surveyed 250 organizations in Australia. The organizations were small to medium sized and all were users of EDI. The focus was on the associated risks with using EDI. The subjects were one technical executive and one auditor from each firm. There were 40 usable surveys returned, from which the authors concluded that there was a distinct difference in perceived risk levels between subject classes. The auditors perceived the risks associated with using EDI “slightly/high to high risk” while technical executives perceived a “slightly/low to average risk.” The results that are the most relevant for the dissertation study include the rank order of the most significant perceived risks: (1) loss or delay of documents during transmission, (2) errors or alterations introduced into messages, (3) network inter-connection risks, and (4) risks arising from inadequate record retention controls and legal liability. There was no mention of internal or external security breaches in the major risk ranking. Additionally, implementation controls security and risk analysis were ranked fifteenth by technical executives and sixth by auditors out of the 16 possible selections. The lack of concern shown for security issues was further demonstrated by their indication that both the technical executives would depend on existing network controls rather than use periodic security audits. They ranked security reviews, dead last—thirteenth. These results seem to support the position that when EDI is used the perceptions of security risk are not considered business risks and as such are not treated as other business risks by technical executives and

auditors. This study provided substance for the inclusion of internal/external connectivity as a dimension of the IT posture construct.

A significant number of security related surveys identify intentional (people instigated) threats as the greatest concern for security practitioners. Furthermore, these threats are more of a concern from employees than from people outside of the firm. Numerous studies have identified employees as the major precipitators of threats to the IT resource and in some cases the most vulnerable aspect of the IT resource (e.g., Edwards, 1994). Kabay (1993) has compiled a list of 35 recommendations for the successful implementation of information security policy based on psycho-social factors. The recommendations stress that constituent involvement is the most important ingredients required for a successful SRM program and that the context and the contents of the messages transmitted and received are critical.

2.5 The Conceptual Research Model

The conceptual research model (see figure 2) draws heavily from the Shirani, Aiken and Reithel (1994) Conceptual Model for user Information Satisfaction (see figure 3), the Suh, Kim and Lee (1994) Discrepancy Model of End-User Desires (see figure 4), the Jarvenpaa and Ives (1991) empirical testing of three models of executive involvement and participation in the management of IT (see figure 5), and the DeLone and McLean (1992) Model of IS Success.

The concepts, constructs and dimensions of the reference models have been adapted and modified in order to conduct a firm level research study investigating questions relative to the important aspects of the process that lead to SRM program effectiveness. Additionally, it is suggested that two distinct models of SRM programs anchor a bi-polar continuum and that SRM programs can be identified along the continuum. Finally, regardless of the actual performance of the existing SRM program countermeasures, the SRM program can be results of research studies using the model should help security practitioners and managers

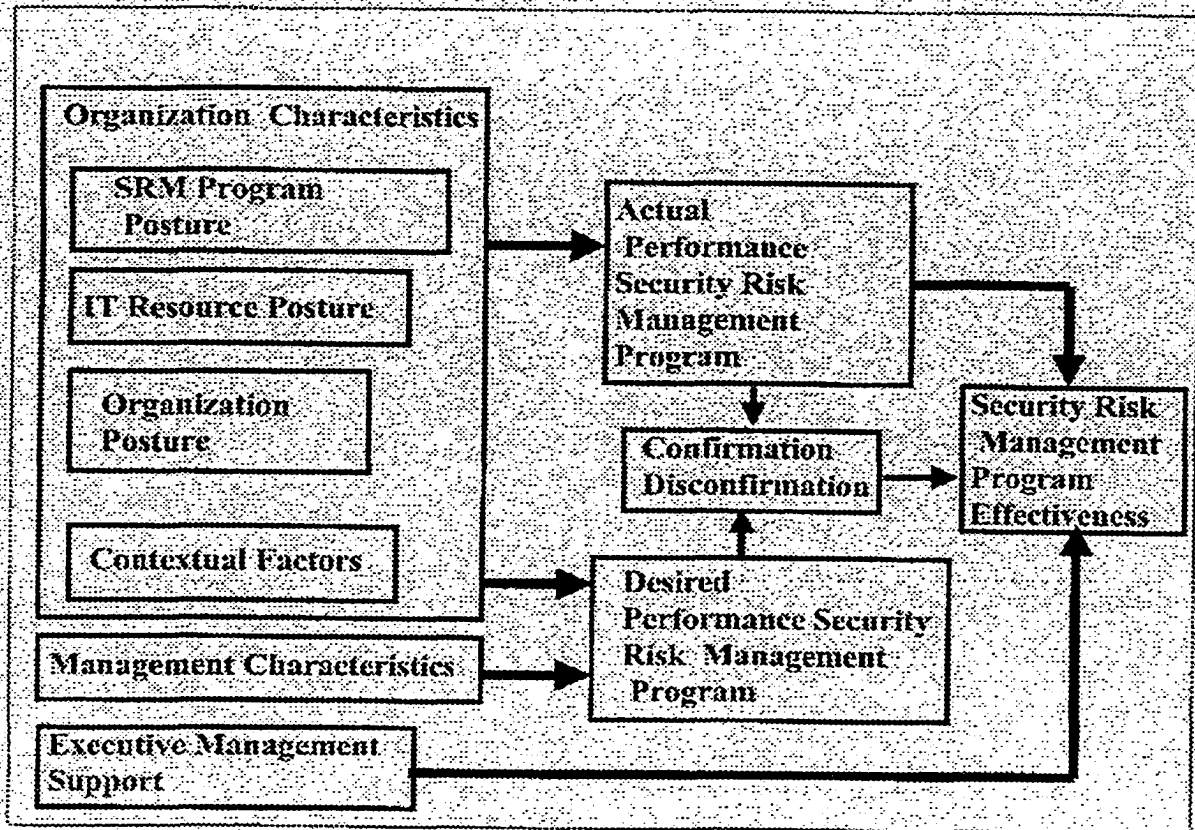


Figure 2. Conceptual Model of SRM Program Effectiveness.

develop and maintain more effective SRM programs. A fundamental underlying premise is that the conceptual research model in no way includes any attempt to differentiate between individual mental or psychological states (Kappelman 1995).

2.6 Organization Characteristics

The organizational environment has been conceptualized as containing external elements that constitute the social and material sectors that affect an organization both directly effective. The model has been operationalized to study SRM issues at the firm level and indirectly (Hatten, Schendel & Cooper, 1978; Schendel & Patton, 1978). Based on this concept, the theoretical concepts of an organizational environment as viewed in organizational theory

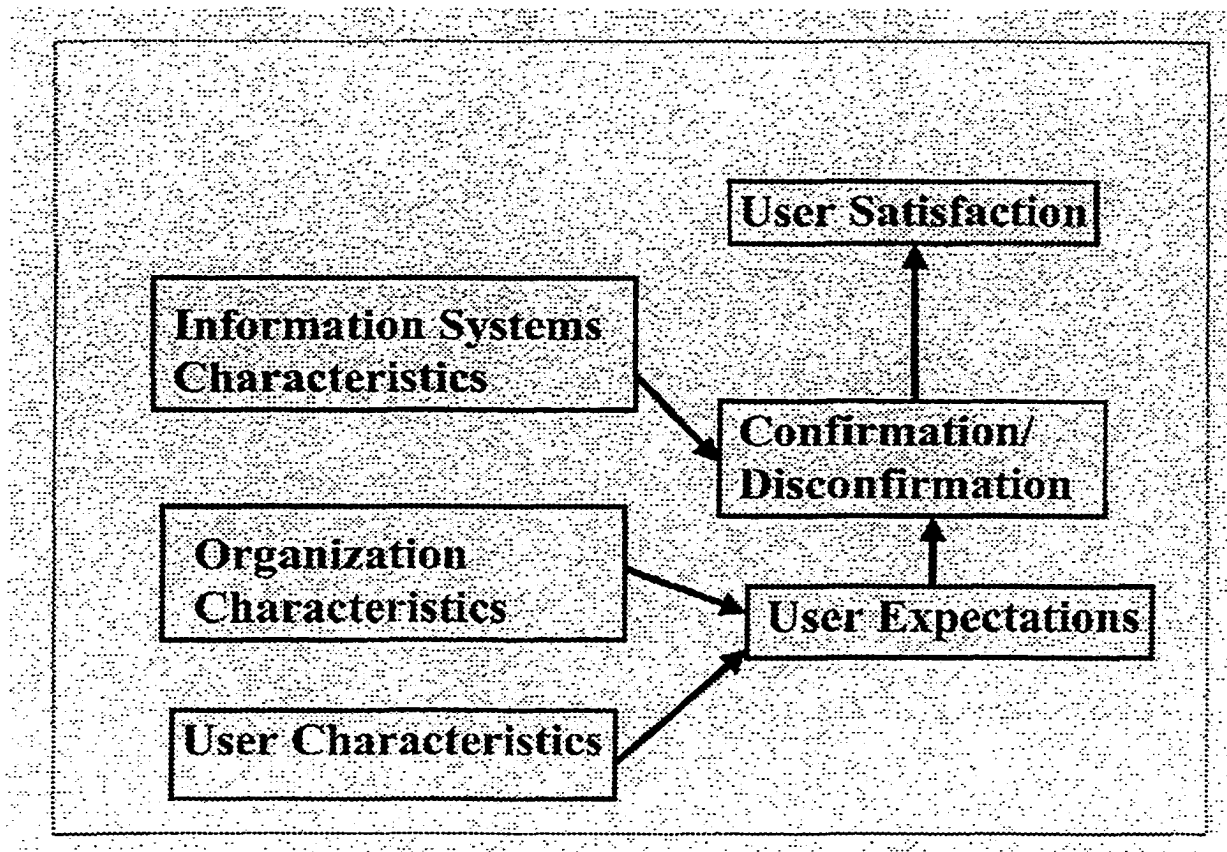


Figure 3. A Conceptual Model for User Information Satisfaction.

research and business strategy research have converged into three major research perspectives (Huber & Daft, 1987). The resource dependency perspective (Hannan & Freeman, 1984), the closely related interorganizational relationship perspective (Porter, 1985), and the information processing perspective (Galbraith, 1974; Tushman & Nadler, 1978; Huber, 1982). The environment being viewed as concrete, external to an organization was the generally accepted position when the environment was discussed (Thompson, 1967). The contingency organization theorists emphasized the importance of the perceived environment rather than the objective environment (Duncan, 1972). Bourgeois (1980) summarized the main ways that discussions of the environment had occurred in the organizational theory literature, outlining

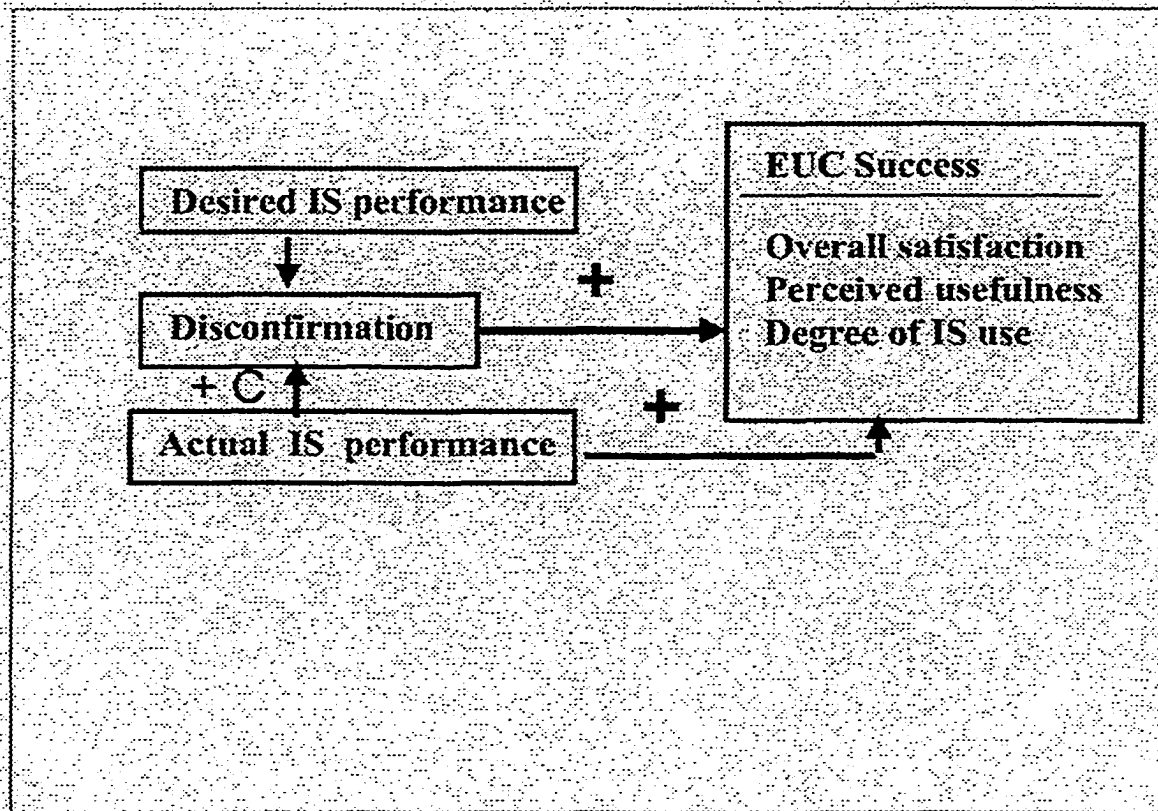


Figure 4. A Discrepancy Model of End-User Desires.

the perspectives taken for conceptualizing the environment (external: objects; external: attributes; internal: perceptions) and the dimensions and how they had been operationalized. Additionally, there are other classifications that have been proposed in the literature. Some have proposed environments that have been identified as objects, perceived, and enacted. This perspective advocates the notion of the enacted environment that was developed in two fields, organization (Smircich & Stubbart, 1985) and cognitive social psychology (Weick, 1979). This perspective emphasizes the importance of managerial interpretation and strategic choice. Management will self-enact their organizational environments, it will not be a given. "If people want to change their environment, they need to change themselves" (Weick, 1979, p. 79).

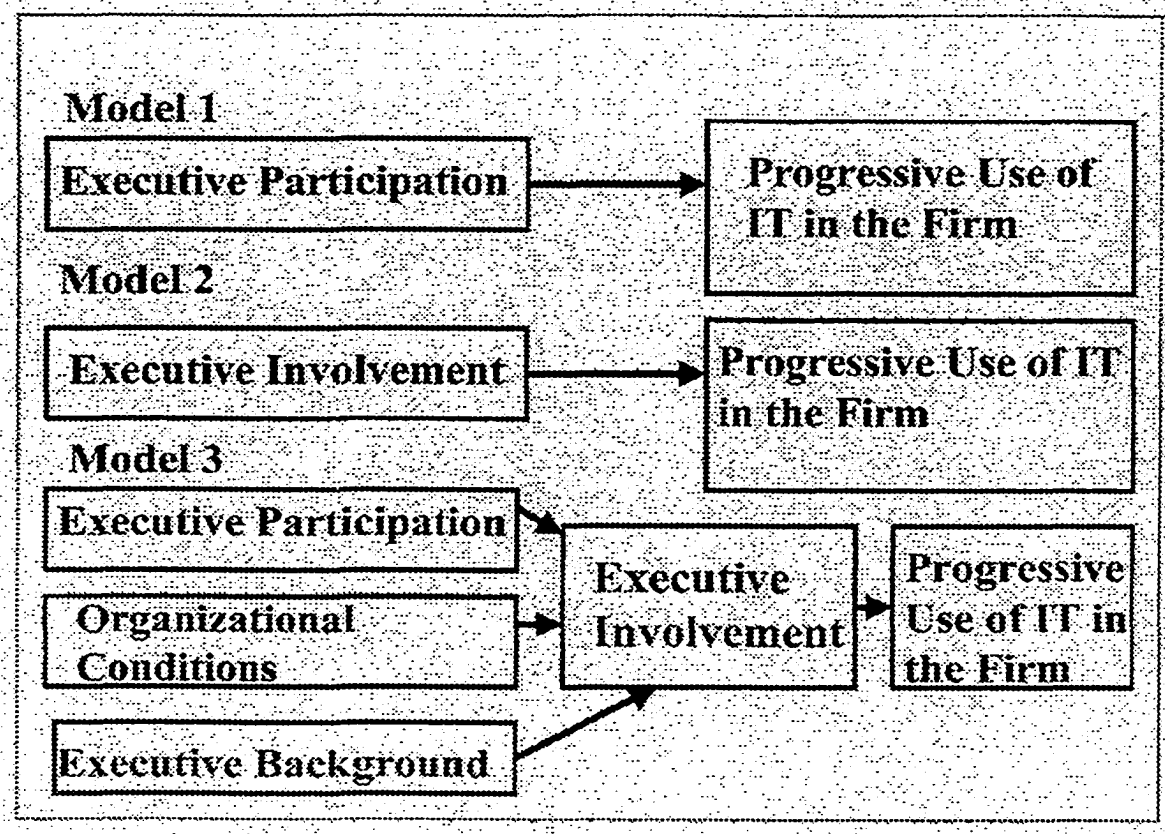


Figure 5. Alternative Models of Executive Source.

The research study uses the notion of the enacted environment within the context of the information processing perspective emphasizing the importance of management interpretation and strategic choice. Simply stated, the TMT of organizations is responsible for obtaining information required for the strategic decisions that all organizations are required to execute (Daft & Weick, 1984). These managers collect and interpret data and information from many different internal and external sources. Therefore, the perceptions they form from this processed information can be used to help in analyzing the actions of these organizations (Cyert & March, 1963; Mintzberg, 1978). The potential level of the utilization the IT resource versus its capabilities will have a direct influence on the security requirements for the organizational information base. With the increased usage of IT resources for strategic purposes the

applications introduce potential higher levels of business and security risks (Lightle & Sprohge, 1992). The perceptions the TMT form about the potential security risks associated with the relationship between the deployed IT resource and the task environment will influence what they desire from their SRM program.

2.6.1 Organization Posture

A useful way to describe traditional organization structure has been to use one of the major ways that have been developed in organization and strategy research to capture the dimensions of organization. Formalization, integration, and centralization have been identified as being among the most consistent (Miller, Drouge & Toulouse, 1988).

In reviewing the reported occurrences of new types of networked organizations, at least four forms have been identified. They are the products of the evolution from mechanistic to organic forms (Burns & Stalker, 1961; Hage, 1988). Namely, network (Lawrence & Davis, 1978; Prahalad & Doz, 1981) modular (Tully, 1993); horizontal (Byrne, 1993); virtual (Byrne, 1993a) and boundaryless (self-renewing) (Devanna & Tichy, 1990). Powell (1992), contends that due to social, economic, technical and managerial factors, the dynamic of team-based organization has moved organizations beyond their boundaries. Therefore, any attempts to identify them using existing “techniques” will fail. The author provides several characteristics that have many overlapping similarities to several of the other so-called emergent organizational forms. The spherical form identified to have overlapping characteristics with other identified emergent organizational forms being reported. This form is suggested as the appropriate required shape to cope with the availability requirements of internal resources being imposed by the stakeholders involved in networked organizations (Miles & Snow, 1995). The authors further suggest that there are other major organizations today that are evolving into full spherical organizations such as Nike, Motorola and Asea Brown Boveri. Based on the descriptions of these spherical organizations, it would seem that flexibility rather than fit would

be the appropriate design criteria emphasized for the security posture of these organizational forms.

There appears to be a major underlying theme that can be detected in the description of the organizational form that will be successful in the twenty-first century (Stewart, 1992). By definition, learning will be the pivotal principle of organizations (Cohen, 1991; Nonaka, 1991; Quinn, 1992). The lack of a hierarchy and functions to collect, evaluate, and pass on information will be replaced by an advanced information technology structure/platform (Glazer, 1993; Keen & Cummins, 1994; Madnick, 1991). These same technologies will facilitate the flow of core knowledge required for the networked knowledge based corporation to function effectively (Huber, 1991; Rockart & Short, 1991; Tapscott & Caston, 1993), processes rather than functions will be the focus of the management process of these networked organizations (Daft & Lewin, 1993; Charan, 1991; Davidson, 1993); firms will move from outsourcing to insourcing creating internal markets (King, 1995); the dynamics of the global environment will require collaborative strategic alliances between the firm, suppliers, customers and even sometimes competitors (Prahalad & Hamel, 1990). The firm will have a dynamically changing external boundary that will include a varying set of constituents (Konsynski, 1993; Ohmae, 1989). If they exist, Internal boundaries will become more open and permeable (Dess et al., 1995). They will be ambiguous bodies that carry within them the potential for major loss of control business risks (Powell, 1992). They will be examples of organizational collectives (Astley & Formbrun, 1983).

2.6.2 Contextual Factors

A major premise in organization science has been the concept of fit. Thompson (1967) postulated that organizations must exhibit characteristics of internal fit or that their processes and organizational structures must be internally consistent and they must be suitable to contend with key environmental contingencies. Nadler and Tushman (1980) defined fit as “the degree to which the needs, demands, goals, objectives, and structure of one component are consistent

with the needs, demands, goals, objectives, and structure of another component” (p. 40). Additionally, organizations must achieve a fit between their organizational elements (structure, process, systems and people) or performance will suffer (Galbraith & Kazanjiam, 1986; Venkatraman, 1989). In organizational research, the approach has been used for rich research streams at the organizational level and has also been suggested for uses at the group and individual level of analysis (Meyer, Tsui, & Hinings, 1993). The theoretical basis of the concept is the ideal type. However, Miller (1992) reported empirically derived results that “organizations that achieve the best fit with environmental uncertainty have the weakest linkages among structural and process variables” (p. 159).

In strategic management and organization the concept of fit or congruence plays an important role in evaluating the performance of organizations. The classic paradigm of strategic management is that strategy, structure and environmental matches or their nonalignment influences the performance of organizations (Rumelt, 1974). Furthermore, the strategic decisions that are made and how they are made have a direct relationship with strategy and environment and therefore influence performance through organization (Shrivastava, & Grant, 1985). Various portions of these configurations have been a subject of much research effort in strategic management (e.g., strategy and structure [Miller, 1986; 1987b], strategy making and structure [Frederickson, 1984; Miller, 1987c], environment and strategy [Miller & Friesen, 1983; Miller, 1987; Venkatraman & Prescott, 1990], environmental fit and internal fit [Miller, 1992; Miller & Friesen, 1980]). However, it must be also understood that not all organizational levels are appropriate for a particular research issue (Castrogiovanni, 1991).

The concept of fit and its importance in studying IT and organization has received major attention in the IS researcher community (e.g., Chan & Huff, 1994; Jarvenpaa & Ives, 1994; Henderson & Venkatraman, 1992; Sambamurthy, Zmud & Boynton, 1994). In the formulation of the original strategic alignment model, Henderson and Venkatraman, (1992) made no mention of the importance of security in the four domains of the model (Business Strategy, I/T

Strategy, Organizational Infrastructure, I/S Infrastructure and Processes). Additionally, in a series of research studies that have investigated segments of the Henderson and Venkatraman model of Strategic alignment none were found that addressed SRM as a dimension of strategic alignment (e.g., Henderson & Venkatraman, 1993).

Jarvenpaa & Ives (1994) adopted a contingency approach and view fit and flexibility as complementary to each other for designing IT configurations (gestalts) in MNCs. They stress the importance of the external/internal fit perspective in that “flexibility should be emphasized over fit when an organization faces a highly turbulent environment or where a firm has built a strategy addressing conflicting competitive forces”(pp. 28-29). These suggestions are similar to the conclusions reached by Miller (1992) relative to the results of an empirical study of organizational environmental fit versus internal fit considerations. A major conclusion was that organizations that exhibited the best external fit also exhibited the lowest levels of internal fit.

A major premise of the proposed research study is that there is a direct relationship between the business risk level associated with the task characteristics of the firm and the current firm level concerns about security risk (SR). It is the threats, vulnerabilities and countermeasures resulting from the fit between the task characteristics and organizational factors that determine the performance of the existing SRM program. If there is a lack of communication between management and the security function, the overall SRM program effectiveness may be negatively impacted both directly and indirectly. In a recent study, Papp and Luftman (1995) found evidence that there is poor communications between general business executives and IT executives relative to business and strategic IT alignment.

2.6.3 IT Resource Posture

The technical capabilities of the IT platform and how they have been utilized by business organizations have been an ongoing area of IS research concern for decades. However, the platform had generally been viewed as being comprised of separate technologies rather than an integrated IT resource (Keen, 1991). There have been theoretical frameworks

and models that view the IT resource in a broader context. Several major ones include Madnick (1991), a theoretical basis for viewing the IT platform in terms of Environmental factors and IT factors which may lead to different levels of connectivity; Applegate & Elam (1992), a framework developed to capture potential organizational impacts of IT; Porter & Millar (1985) and Venkatraman (1994), framework to capture the role of the IT platform within the context of strategic issues. The dissertation will adopt the concept of the IT resource and its role in both supporting the generic business strategies and also in performing organizational tasks. The definition used for the proposed research study is: The IT Resource Posture of an organization includes all of the technologies, capabilities and data and information and how and why they are being deployed inside the organization or external to the organization.

2.6.3.1 Electronic Integration (EI) Level

The EI level has been identified as a dimension that can help to position a firm's level of potential security risk. The Venkatraman (1994) model of Electronic Integration identifies the role of business networks linking enterprises along a continuum of the "unstructuredness" of the information being transmitted over the linkages. The range extends from low (transactions) to high (knowledge). The model captures the concepts of "connectivity" and "the networked business organization." The concept, dimensions and nomenclature have been incorporated in instruments used in several empirical research studies. Additionally, the Venkatraman framework also includes the governance aspect of the level of EI being used and therefore in the conceptual research model IT resource posture has been operationalized using EI Level a dimension.

2.6.3.2 Reach and Range

The IT resource posture dimension has been partially captured by Keen (1991) in the seminal work on the reach and range of the IT Platform. The reach and range measure and measurement methodology adopted for the dissertation is based on the theoretical model

developed by Keen. The reach and range of the IT Resource will be one of the measures of IT resource posture. The reach/range measure will capture the utilization and capability aspects of the IT deployed resource. The Range is defined as the level of information that is accessible across the IT platform. The Reach is defined as the level of connectivity of the IT platform.

2.6.4 Security Risk Management Program

The dimensions of the SRM program construct are not based on empirically derived research findings. A content analysis was conducted on practitioner security literature published after 1980 to extract reoccurring major suggestions about what should be included in a corporate level SRM program (see table 2).

It was proposed that four major dimensions could be developed to capture the overall posture of an individual firm level SRM Program. The dimensions are: (1) governance, (2) countermeasures, (3) structure, and (4) policy and procedures. Furthermore, it was proposed that different models of SRM programs could be identified and that any can lead to effective SRM programs. The SRM program construct has been operationalized using the concept of posture as the surrogate. The measures have been selected to position the posture along a hard < > soft continuum based on positioning the measures according to the following criteria: (1) governance—centralized/shared/distributed, (2) countermeasures—reactive/pro-active, (3) structure—centralized/decentralized, and (4) policy and procedures—formalized/casual. This approach is similar to what has done relative to predicting business performance/effectiveness using the Miles and Snow typology (Hambrick, 1983; Doty, Glick & Huber, 1993; Shortell & Zajac, 1990, Zajac & Shortell, 1989).

2.6.4.1 SRM Program Governance

The governance (What and How) of the SRM program posture measure should be a suitable measure to capture the essence of the scope of the administration requirements for the SRM program. The measure has been extracted from the evolutionary literature on SRM

programs (Hitchings, 1995). The measure captures the range from Fully Centralized, Shared, to Fully Decentralized. The governance of the security required for the IT resource may be centralized or there may be shared responsibilities between the central authority and the individual user or functional group (Bergeron & Berube, 1990). Additionally, the governance of the security required for the IT resource may be under the management of people who lack the level of technology training required to manage the technology (DeMaio, 1995a). Finally, the governance of the security required for the IT resource may be totally distributed to the individual user or functional groups (Frank, 1988; Tipton, 1994).

2.6.4.2 SRM Program Countermeasures

Generally, the commonly held definitions of countermeasures all seem to mirror how Eloff et al. (1993) define it, "The main deliverable of a risk analysis study is the identification of countermeasures for threats identified" (p. 598). This definition offers a limited perspective and a more holistic perspective has been adopted. The definition of countermeasures used for this research study is: The array of organizational devices that are included in the existing SRM program that may deter, prevent, or detect security breaches.

Today, there are several major new families of countermeasures being suggested that should be considered by organizations as necessary additions to their current portfolio of security countermeasures. Some of the recent major ones being discussed are: penetration teams using new tools such as security analysis tools and social engineering, security quick reaction teams, and accessing Internet security site-related resources.

An example of a recent addition to the available countermeasures that can be utilized by either the group responsible for the security or governance of the IT resource or by a penetration team is the Security Analysis Tool for Auditing Networks (SATAN). The software was developed for detecting vulnerabilities in LANs, clusters of LANs and WANs that may or may not be connected to the Internet via an in-house mainframe or client/server architecture. The SATAN software package scans for configuration errors and can list and/or investigate

what the vulnerabilities are. There has been considerable controversy surrounding this countermeasure as to its being a help or a hindrance to security practitioners. The easy access to the tool has been cited as a potential boom to the hacker community, and it has also been reported that one of the authors was fired for posting it on the WWW (Doty, 1995). There are other tools readily available for the same type of network analysis, ISS and pingware being amongst the most popular and commonly known.

Recently, it has been suggested that “social engineering” be added to increase the potential for discovering vulnerabilities that have not been discovered by prior penetration techniques. As described by Ceraolo (1996), “Social engineering requires building trust with [company] employees or a commanding, even intimidating, presence of authority” (p. 37+). Applying social engineering as a part of penetration team techniques focuses on the human factor and can possibly be a dysfunctional technique if not handled properly

Today organizations are forming security related special response teams. In general, these quick reaction groups are being set up to deal with organizational computer related security problems. The idea is for the team to collect current information about possible security related issues (i.e., security related software bugs, hardware problems, new potent viruses, worms) and then to disseminate appropriate information internally in the organization. The unit is usually responsible for identifying and assisting in dealing with all organizational security breaches. The individual organizations can elect to join the Computer Emergency Response Team (CERT) system that is administered by the National Institute of Standards and Technology (NIST). The NIST is the governmental agency responsible for computer science and technology activities within the U.S. Federal Government. The institute has many activities that are available to the private sectors of the economy. Their Computer Security Resource and Response Center (CSRC) runs a 24-hour telephone hotline and a BBS. A well-known quick response team was formed because of the growing security concerns of the research community using the Internet. Their concern prompted the formation of the Computer

Emergency Response Team/Coordination Center (CERT/CC) by the Defense Advanced Research Projects Agency (DARPA) in 1988. The CERT/CC has been operating as a central hub for Internet computer security related issues with the vendor, user and security practitioner community. The CERT/CC is located at Carnegie-Mellon University (CMU), and it is managed by their Software Engineering Institute (SEI). Recently, the CERT group at Carnegie Mellon University started signing up organizations that will utilize their CERT group to respond to security breaches, and provide training and general consulting for information security. Currently, the group provides free incident reports to the general public ("Edupage," 1996). Another well know group is the Computer Incident Advisory Capability (CIAC) which is the computer incident response team for the U.S. Department of Energy and the National Institute of Health. CIAC is one of the founding members of the Forum of Incident Response and Security Teams (FIRST). The concept behind FIRST is to foster cooperation and coordination of the globally expanding network of computer response teams ("Risk Digest," 1996). There are many new sites appearing on the web that are easily accessed in order to gain security related information. Many universities and colleges now have home pages for their security related ventures such as Computer Operations, Audit, and Security Technology (COAST) at Purdue University. The site is an excellent source for security related information and offers other security related links. These new types of countermeasures are proactive measures that are suitable for a soft posture SRM program.

2.6.4.3 SRM Program Structure

It has been suggested that due to the heightened levels of overall environmental "risk," (i.e., financial, technology, governmental [environmental, occupational safety], operational disaster, insurance) resulting from the expanding task environment of organizations, a corporate risk function, will be a necessity (Highland, 1993). Similar to the IS function, the security function should be located at a high level in the firm in order to align its organizational goals with the overall strategic goals of the firm. Additionally, the security function must have

working and effective relationships with all functions and all levels of the organization. The structural imperatives identified for IS organizations may be necessary for an effective security organization (Rockart, Earl & Ross, 1996).

2..6.4.4. Security Policy and Procedures

Today there are claims that there is general agreement that organizations need a “security policy”(Lindup, 1995, Sterne, 1991). However, exactly what should be included in security policy seems to an elusive aspect of SRM programs. An extensive search of the practitioner literature was conducted in order to isolate and identify major areas that have been suggested that should be included in corporate/firm level security policy and procedures (see table 2).

There is major disagreement as to the requirements for a written security policy for organizations that encompass aspects of the new emergent organization forms. There are several conflicting suggestions that these new types of organizational forms should and should not have a formal written security policy. Furthermore, what should or should not be included in their security policy and what type of security governance should be utilized. Additionally, that due to the interconnected more open systems these more organic forms are taking the emphasis should be on relying on advanced technology applied at a higher level of authority due to a general loss of central coordination and control.

2.7. Management Characteristics

The characteristics and dynamics of the top management team (TMT) have been a subject of interest for both theoretical and empirical research in organization and strategy. There is a strong theoretical and empirical basis for focusing on top management team characteristics and their influence on content and process issues and the role of the group dynamic in the SRM program decision making process. The importance of these has been empirically demonstrated in the business strategic decision making process and what their

influence is on organizational performance (Chakravarthy & Doz, 1992; Hambrick, 1987; Hambrick & Mason, 1984).

In strategy formulation theory and research there have been two major streams that have developed: the strategy content school and the strategy process school (Andrews, 1980; Ansoff, 1965; Huff & Reger, 1987; Pettigrew, 1992). The TMT has received much attention in the process stream. There have been studies that have investigated the TMT and the SMP within the context of environmental and structural fit (Koberg, Tegarden & Wilsted, 1992; Priem, Rasheed & Kotulic, 1995), the political context (Cyert & March, 1963; Eisenhardt & Bourgeois, 1988), the role of consensus (Bourgeois, 1980, 1985; Dess & Origer, 1987; Priem, 1990), and TMT demographics (Eisenhardt, 1989a; Hambrick & Mason, 1984).

There is mixed evidence on the role of information availability and effective decision making. Some research results support the position that the TMT will rely on what is known and will not seek new information during the SMP regardless of the environmental context (Wang & Chan, 1995). An excellent review of empirical research on strategic decision process uses an integrative framework in order to identify and clarify conceptual issues and relationships used in empirical strategy process research (Rajagopalan, Rasheed & Datta, 1992). The authors extracted two broad conclusions from their evaluations:

First, strategic decisions are made in the context of two sets of factors: (1) an organization's environment in terms of its complexity and volatility and (2) organizational conditions such as the internal power structure, past performance, past strategies, and the extent of organizational slack.... Second, even within a single organization, the process varies across decisions. (p. 4)

2.7.1. Decision Making Under Uncertainty

In his seminal work Raiffa (1968) reported on the results of a simple question asked of two experimental psychologists. Their question was simply what was the least amount of money either would take to give up the rights to a lottery ticket, which gave a 50–50 chance to win either \$0 or \$1,000. The dramatic differences in their answers \$50 and \$450 led Raiffa to

make a recommendation, which had a direct influence on the progress of the proposed research study.

But if we are to advise each of them how they should behave in a decision problem similar to the one posed to you, then we had better simply accept the fact that they differ in their attitudes toward risk and that these differences will influence their choices. (p. 52)

Can these conclusions reached by Raiffa be one of the major contributing factors relative to apparently reported misalignments between organization postures and organizational security postures? Are there differences in managerial attitudes and perceptions towards security risks versus other types of business risks, and are these influencing management choices relative to the appropriate security measures required for the deployment of the IT resource? Are there differences in attitudes held by managers who can be classified as risk takers or risk avoiders relative to business and security risk? Furthermore, can we identify how these attitudes are influencing their SRM program choices?

The risks managers must contend with are perceived risks. The TMTs of organizations are making these decisions based on what their perceptions are about the effect the “likely” consequences will be of their decisions. They do not trust or use probability estimates in their decision making processes (Fischhoff, et al., 1981; Slovic, 1964). They may not recognize what some of the outcomes may result in relative to the security posture of the organization. They may hold concepts about the outcomes, which are totally wrong relative to the likelihood or severity of the outcome. Some managers may perceive outcomes that have no basis in reality (Wharton, 1992). Therefore, perceived risks should be a paramount issue when conducting research studies associated with decision making in general and specifically the decision making process relative to the formulation (contend and or process) of security policy decisions.

2.7.2 Risk Attitudes and Perceptions

In the field of decision theory and individual attitudes towards risk, there are at least four theoretical research streams that exist. March and Shapira (1987) reexamined the collective research studies available at the time relative to managers' risk taking strategies, and they concluded that any research studies that focus on how company management defines risks and their reactions to risk should draw from the collective works in the fields of behavioral studies of organizational decision making (March & Simon, 1958; March & Shapira, 1987), behavioral decision research (Nisbett & Ross, 1980; Kahneman, Slovic & Tversky, 1982), and the behavioral assessment of risk perception (Slovic, Fishhoff & Lichtenstein, 1986).

There is also the traditional decision theory school which posits that larger expected returns are preferred by decision makers, holding all other factors constant (Lindley, 1973). Furthermore, decision makers are risk adverse (Ross, 1981). However, in the behavioral school Slovic (1964), after an extensive review of the extant literature both theoretical and experimental, postulated that risk attitudes are context specific and that risk is a multidimensional concept. March and Shapira (1987) have also leveled this criticism against the traditional decision theory school. Since Slovic first postulated the concept that risk attitudes are context specific there has been an empirical research stream that has grown in prominence as the topic of public risk issues associated with health, safety and the ecology has grown in importance on the national scene.

2.8 Risk Perceptions and the Psychometric Paradigm

There has been a gradual movement in perspectives relative to how perceptions of risk are being viewed in the decision making process. Currently, the shift has been to draw heavily from the work of Wallsten (1980) in the field of cognitive psychology. This perspective is dominant in the study of perceptions of risk and the management of risks in the public sector, especially in safety and ecological risk.

In the fields of health and safety there has been a rich research stream of descriptive studies that focus on how individuals perceive risk and /or how they evaluate risk reduction proposals (Fischhoff, Slovic, Lichtenstein, Read & Combs, 1978; Slovic, Fischhoff & Lichtenstein, 1982; Borchering, Rohramann & Eppel, 1986). Additionally, research studies have been conducted in the ecological risk domain using the psychometric paradigm (McDaniels, Axelrod & Slovic, 1995). In both cases the fundamental questions are related to managing risk. The focus of risk management in these fields has shifted to individual risk perceptions.

The early factor analytical works by Slovic, Fishhoff, and colleagues are the prominent seminal works in the psychological literature on individual risk perception (Sparks & Shepherd, 1994). Slovic, Fishhoff and colleagues conducted experimental research studies in order to identify the characteristics influencing what people perceive about risks associated with technology. They adapted the psychometric scaling methodology for these early works. Slovic (1964) conducted an extensive review of the research work done to date related to risk taking behavior in several different types of research streams. Slovic identified one major cause of why there was a lack of consistency amongst measures being used that “tapped” the construct of risk taking. “Risk taking behavior appears to be multidimensional in nature. It has substantial subjective components and is susceptible to a variety of motivational and other influences” (Slovic, 1964, p. 231).

The model that was developed by Slovic, Fischhoff and Lichtenstein, (1986) and Slovic, (1987) has been the model used extensively in studies investigating risk perceptions in the health and safety field. The Slovic model is based on the nine dimensions of risk that were suggested by Lawrance, (1976). Namely, voluntariness—degree to which the activity is voluntary, dread—degree to which the negative consequences of the activity are dreaded; control—degree to which the person engaging in the activity has control over the consequences; knowledge—degree of knowledge the person engaging in the activity has about

the associated risks; catastrophic potential—worst-case disaster severity of the activity; novelty—degree to which the activity is new or novel or old and familiar; equity—degree to which the consequences of the activity are fairly distributed.

The dissertation will use the concept of the multidimensionality of risk as theorized and experimentally demonstrated by Slovic and colleagues has been incorporated in the operationalization of the SR knowledge and SR awareness dimensions and also in the risk propensity dimension of the firm management characteristics construct.

2.8.1 Risk Attributes

Slovic (1987) summarized “risk perception school” research to date and identified various clusters of attributes that describe how people perceive technological hazards and risky behavior. The risk perception research stream he summarized attempts to explain why people frequently reject the findings of studies that have been conducted to aid policy decisions relative to managing environmental risks. The first factor he identified was dread. Risks are perceived as potentially severe, uncontrollable, and catastrophic. The second factor is identified as knowledge, the risks associated with the perceived level of knowledge or lack of knowledge about a hazard. The risks are perceived as unknown when they are new or unfamiliar, are involuntarily imposed, and have delayed effects. The third factor identified is risk exposure, the level of perceived exposure to a risk. This factor has both personal and societal levels of exposure.

2.9 Risk Awareness and Knowledge

Maharik and Fischhoff (1993) found in a series of studies that, in general, the more that people know about the risks of using a technology, the more favorable they are. Exceptions were pro-technology people and anti-technology people. A key finding was that the technology being investigated cannot be something that elicits extreme polarized responses for or against the technology from these two extremist groups. The first study used open-ended interviews

that assessed beliefs regarding the risks of a single technology. The results showed that knowledge/attitude correlated with activist and non-activist individuals. The second study investigated individual knowledge levels and whether they were based on realistic or non-realistic concepts. The correctional results suggest that increasing peoples' knowledge towards a technology seemed to make them accept it more.

Metcalfe and Powell (1995) developed an alternative perspective to how individuals handle information that differs from the transmission perspective developed by Shannon and Weaver (1949). The transmission perspective had been the dominant perspective used for Information Systems research. Metcalfe and Powell (1995) postulated as part of their proposed alternative "perceiver-concerns perspective" that

because a person has concerns, it does not follow that she or he will actively seek information. It only means that the concerns will influence the information content he or she will extract from a message.... Even, if the level of concern is high, the pro-active seeking of information is not ensured. (p. 127)

2.9.1 Business Risk Propensity

In an empirical research study, MacCrimmon and Wehrung (1990) surveyed 509 top level business executive subjects from U.S. and Canadian firms to determine the validity of commonly held concepts about socio-economic factors related to risk takers and risk avoiders. The main research question was whether there are systematic differences between risk takers on socio-economic dimensions. The authors developed three types of risk propensity measures based on questions derived from theories of risk using standardized situations; revealed choices in naturally occurring situations and attitudes towards taking risks. The authors used multi-methods to examine the reliability and validity of the measures. The inter-item reliability was also judged to be adequately high. The authors were able to construct risk measures for 90% of the respondents. The authors constructed socio-economic factors in a similar manner. They used linear multiple discriminant analysis to construct linear combinations of the socio-economic factors in order to test whether any would significantly discriminate between the

most risk adverse executives and the most risk taking executives on specific risk factors. The authors concluded: (1) no single measure of risk propensity is adequate to capture the complexity of risk taking behavior and (2) no single category (set) of risk measures could predominate in discriminating between risk takers and risk averters based on socio-economic characteristics. However, the authors did not consider the influence of beliefs on the executives' attitudes towards risks, which may influence their individual and collective behaviors (Ajzen & Fishbein, 1980).

MacCrimmon and Wehrung, (1986) conducted a survey of 2,720 executives in the United States and Canada. The study had an overall response rate of 18.7%. The study was conducted via self-report questionnaires, and due to a low initial response rate they conducted interviews with executives who did not respond to the original mailing. They used decision scenarios based on an in-basket booklet where the executives were requested to respond to hypothetical situations. The study also included questions about the executives' attitudes towards risk. The executives were also asked to make decisions about investment gambles. A major conclusion was that the executives avoided risk and that they delegated these risky decisions to others.

Fredrickson (1984) conducted a series of research studies of the strategic decision making process in several industries. In discussing the results of the 1984 study he indicated that the characteristics of the firms' strategic processes exhibited patterns. Furthermore, he noted that the patterned behavior of individuals is what makes one organizations process more comprehensive and another organizations less. These conclusions are in line with the findings of a series of studies conducted by Mintzberg and colleagues (Mintzberg, 1978; 1987; Mintzberg & McHugh, 1985; Mintzberg & Waters, 1982, 1985). They found that through the process of classifying decisions that consistent patterns could be identified that identified the realized strategy of the firm. The effective decision-maker must focus on the aspect of the decision that has the greatest impact and risk to the overall strategic goal (Lamkin & Courtney,

1995). The patterns of decision-making exhibited during the SMP activity of organizations should have a major impact on the decision-making patterns executives use to establish the SRM program posture of organizations.

2.9.2 Security Risk Propensity

Recently, there has been some recognition in risk management practitioner journals that today, a paradigm shift (viewing the business enterprise as an open system) is required to fully address all of the steps required for risk management (Settembrind, 1994). Furthermore, due to fundamental changes taking place in the global environment, top management must consider (within the same framework) the business risks associated with security breaches similarly to how other business risks influence the organization's market effectiveness (Hill & Smith, 1995). Risk management must not present top management with what the security costs will be to protect against a single business loss due to a single security incident loss event rather than the possibilities of different and multiple security breaches occurring (Fried, 1993). Secondly, Tipton (1994) suggests that personnel liability issues of corporate management associated with their firm's full business utilization of the IT resource should be incorporated in the risk management approach being used by their firms. In fact, Tipton (1994) identifies the scope of the personnel liability issue in a broader context as "unauthorized use of licensed software, archives of obsolete information, lack of adequate disaster recovery planning, inadequate protection against industrial espionage, noncompliance with government regulations, bad data, employee privacy and more" (p. 59). A third consideration should be the nature of the concept of security itself. O'Leary (1995) probably summed it up in a few sentences:

Security is not uppermost in the minds of users or management. Security is usually visible only when messed up or perceived as a detriment.... When security is done well nothing happens...security affects everything else...security can be affected by almost everything else. (pp. 30-31)

Fourthly, the attitudes held by the CEO and the other members of the TMT can have a major impact on the design of the current security risk management program and the desired

performance of such a program. Lewin and Stephens (1994) argued that "micro-level properties of the CEO may be enacted in macro-level features of the organization" (p. 186). Therefore, CEO attitudes relative to risk propensity and trust in people might be important user characteristics that directly influence the desired performance of security risk management programs.

2.10 The Confirmation/Disconfirmation Paradigm

In marketing, the topic, "consumer satisfaction" has received considerable theoretical and research attention. A major portion of the theoretical and research streams has emphasized the process underlying consumer satisfaction rather than the content of customer satisfaction (Tse, Nicosia & Wilton, 1990). Within the process sector a rich research stream has focused on specific determinants of consumer satisfaction. A major section emerged that focused on the expectancy disconfirmation concept (Bearden & Teel, 1983; Churchill & Suprenant, 1982; Oliver, 1980). This stream elaborated on the antecedents trying to capture the richness of the process responsible for how consumers form post purchase expectations (beliefs or predictions) about the performance of a product or service. The model proposed by Oliver (1980) has had considerable attention, and a significant number of empirical research studies have been conducted on portions of the model resulting in various levels of support for the model (Bearden & Teal, 1983; Churchill & Suprenant, 1982; LaBarbera & Mazursky, 1983; Oliver & DeSarbo, 1988; Olson & Dover, 1979; Tse & Wilton, 1988).

The Oliver model suggests that during the customer satisfaction process, consumers form pre-purchase expectations about the performance of a product or service. The pre-purchase expectations are compared with the post-purchase actual performance, which leads to one of three possible results: (1) the expectation and the actual performance do not differ resulting in a confirmation which is a neutral result, (2) the actual performance is greater than the expectation resulting in a positive disconfirmation which leads to satisfaction, and (3) the actual performance is less than the expectation resulting in a negative disconfirmation which

leads to dissatisfaction. In reviewing the IS user satisfaction literature stream two studies were identified that incorporated the Oliver model in the topic of systems success.

The conceptual study by Shirani et al. (1994) (see figure 3) developed a broadly based explanatory model of user information satisfaction. The model incorporates the confirmation/disconfirmation paradigm as developed by Oliver. The authors suggest that the model provides a new approach to understanding the process and variables that are ultimately responsible for user information satisfaction. They provide support for the position that it is important to account for contextual factors and process if one is investigating issues associated with IS success constructs (DeLone & McLean, 1992).

The Suh et al. (1994) Discrepancy Model of End-user Desires (see figure 4) introduced the concept of desired expectations as a substitute for expectation/anticipation in the disconfirmation of expectation paradigm. The researchers demonstrated that the model attitudinal measures of EUC success were significantly influenced by the level of discrepancy. The study used overall satisfaction and perceived usefulness measures as surrogate dimensions for EUC success.

2.11 SRM Program Effectiveness

The Suh et al. (1994) Discrepancy Model of End-User Desires uses degree of IS use as one measure of EUC success. The measure has a long tradition in the IS field being used as a surrogate measure for benefits derived from use of a system. In a comprehensive review of the IS literature conducted by DeLone and McLean (1992), the IS success measures they found were classified into six categories. The resultant IS Model of IS Success they developed from their classification shows Use and User Satisfaction as being interdependent. Seddon (1997) extended the DeLone and McLean model and respecified it to clarify the model and to improve the usefulness of the model. Suh et al. (1994) suggest that when IS Use is used as a surrogate for benefits from use, then success seems to be equated with high usage systems. Based on the work of Szajna (1993) they argue that the "critical factor for IS Success measurement is not

system use, but that *net benefits* should flow from use” (p. 242). This is similar to the situation with a SRM program. The organizational net benefits should flow from the program and therefore this should be an important determinant of the success of the system, which we can use as a surrogate measure of system effectiveness. In the Suh et al. (1994) model, Degree of IS use is used as one independent measure of EUC Success. Due to the above stated reasons this measure will not be used as a surrogate measure for program effectiveness. Additionally, the Seddon (1997) respecified model of the DeLone and McLean (1992) model identify Perceived Usefulness and User Satisfaction as general perceptual measures of the Net Benefits of past IS use. For the proposed research study, perceived usefulness and net benefits will be used as surrogate measures for program effectiveness.

2.12. Executive Management Support

The concept that executive management support is a necessary condition for the successful implementation of IT in an organization has a long history in the IS literature. The extant literature stream contains empirical studies that have specifically addressed the relationship between executive management support and the use of IT in the organization (DeLone, 1988; Yap et al., 1992, Thong, Yap & Raman, 1996). The two major studies that are the foundation for the inclusion of the executive management support construct in the research model are:

1. The empirical study conducted by Jarvenpaa and Ives (1991) that focused on the role of the CEO using three different models (see figure 5). In the study, the dependent variable in each model was the progressive use of IT in the firm.
2. The research study that was conducted by Leonard-Barton and Deschamps (1988) investigating the influence of organizational managerial actions relative to organizational IT usage. The authors investigated the positive and negative aspects associated with mandates, resource allocation, incentives and reward systems on the organizational use of IT.

Based on the evidence that has been presented the following hypotheses are proposed:

H1. Executive management involvement in the SRM program is positively related to the perceived usefulness of the SRM program

H2. Executive management involvement in the SRM program is positively related to the perceived employee compliance with the SRM program.

H3 Executive management participation in the SRM program is negatively related to the perceived usefulness of the SRM program.

H4 Executive management participation in the SRM program is negatively related to the perceived employee compliance with the SRM program.

2.13 Actual Performance of SRM Program

The importance of the performance of security measures is an aspect of security that has received little research attention. There is consensus that it is difficult to cost-justify security related expenditures (Plant, 1993). Furthermore, it is extremely difficult to demonstrate the tangible benefits (performance) of security measures to management. Additionally, only the most recent negative past performance will have a direct influence on management concerns about existing security measures. Wood (1995) suggests that the security organization should prepare and present new policies they want implemented right after a major information security breach, unfavorable computer-related audit report, security-related lawsuit, or some other type of loss which has received extensive top management attention. The actual performance level of systems has been identified as both an important direct and indirect determinant of the effectiveness of IS programs (Shirani et al., 1994; Suh, et al., 1994). Based on the evidence presented in the chapter the following hypotheses are proposed:

H5. The security breach severity level is negatively related to the perceived usefulness of the SRM program.

H6. The security breach severity level is negatively related to the perceived level of employee compliance with the SRM program.

H7. The magnitude of actual security breach costs is negatively related to the perceived usefulness of the SRM program.

H8. The magnitude of security breach costs is negatively related to the perceived level of employee compliance with the SRM program.

2.14 Disconfirmation Gap

The empirical results of the Suh et al. 1994 study demonstrated that the gap that exists between the desired performance and the actual performance of a product or service directly influence the perceived effectiveness of a product or service. Additionally, the reasons why the organizational SRM may not be suitably structured to handle the potential threats and vulnerabilities resulting from the organization task environment were discussed. This was shown to possibly result in actual low performance levels relative to what was desired. The gap (actual vs. desired) may also develop due to differences in the TMT profiles of the firm (awareness/knowledge of security, risk profiles, individual characteristics). The TMT may be aggressive strategic business risk takers and at the same time some of these same managers may not be aware of the level of security risk associated with aggressive strategies that may utilize EI, open systems, distributed computing environments and networked organizational structures. These stakeholders may not consider the risks as relevant due to their individual concerns and or interests (Willcocks & Margetts, 1994). Based on the evidence presented in chapter 2 the following hypothesis is proposed:

H9. The effectiveness of the SRM program is positively related to the level of positive disconfirmation between desired performance and actual performance.

CHAPTER III

ORIGINAL RESEARCH STRATEGY AND METHODOLOGY

3.0 Introduction

Chapter 3 is divided into major sections that include the original research strategy, research population and sample selection process, the research methodology that was to be used to construct and validate the research instruments, the data analysis methodology and the statistical methodology that were planned to empirically test the hypotheses.

The research strategy was revised after the pilot test phase of the research project. There was a significant reduction in the scope of the research model (see figure 6) that was to be tested. The questionnaires that were used for the data collection phase of the research study only include the constructs and relationships included in the revised research model (see figure 7). The tables only include the constructs, dimensions and measures that were included in the revised research model (see figure 7). The details of the actions taken due to the conditions experienced during the pilot test and data collection phase of the research study are explained in chapter 4.

3.1 Research Strategy

The original research strategy included a preliminary field study at two firms that had a security risk management program in place for at least one year. This would insure that they had a mature security culture. The field study was to be used to pilot test and refine the research instruments. Following the administration of the instruments, semi-structured and structured interviews were to take place with the firm managers. The managers were to include the highest-ranking information security and IS official. The focused interviews were to be analyzed using an open coding procedure to screen for the emergence of unanticipated

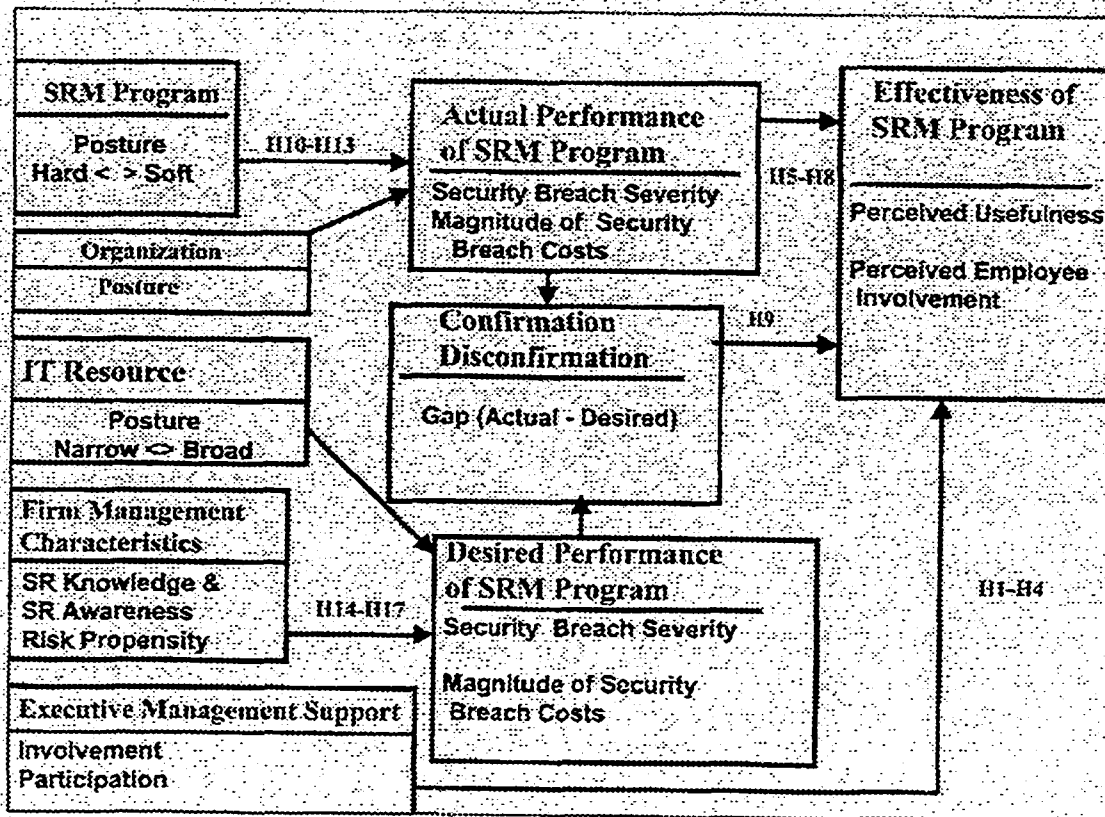


Figure 6. Original Research Model SRM Program Effectiveness.

organizational and managerial characteristics relative to what had been proposed or hypothesized (Spender, 1989; Strauss & Corbin, 1990). Based on the outcome of the two firm data analyses, there was to be additional firm sites used to further refine the construct measures. The finalized research instruments were then to be sent to a sample of firms selected from the total population of firms available. The entire process was to follow the Churchill (1979) research paradigm for the development of construct measures (see figure 8).

3.2 Planned Sample Selection

The initial sample of organizations was to come from a heterogeneous industry population of U.S. firms. Choosing a cross section of industries limits any attempt to associate

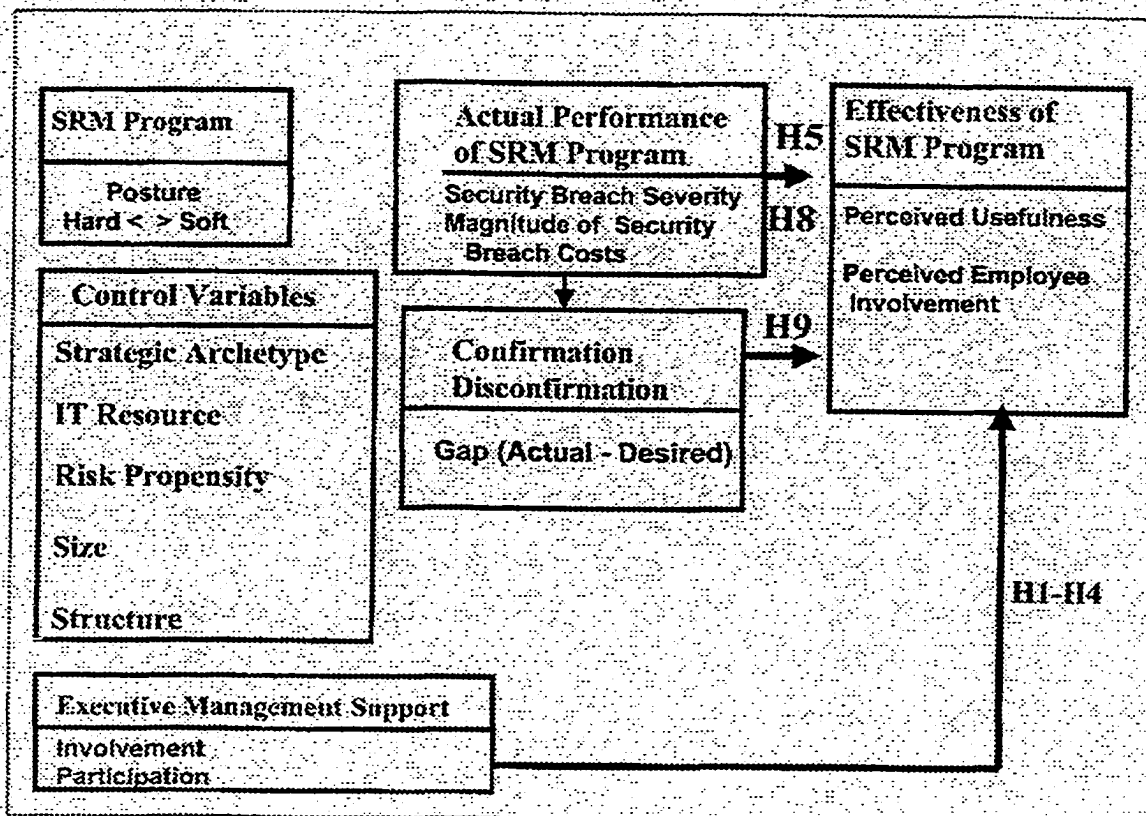


Figure 7. Revised Research Model SRM Program Effectiveness.

the results in terms of applicability to any single industry or organization. The aim was to strive for the maximum level of generalizability as practical with respect to the population and maintain an acceptable level of precision in control and measurement of the variables (McGrath, 1982).

The sample of firms was to be selected from a population of organizations that should have an established security risk management culture (SRM program at least one year). This was planned since the major questions that were being investigated are only applicable with an SRM program in place for one year or longer. The sample of firms was to be drawn from the membership listings of selected ACM-SI groups. The groups were to include the following:

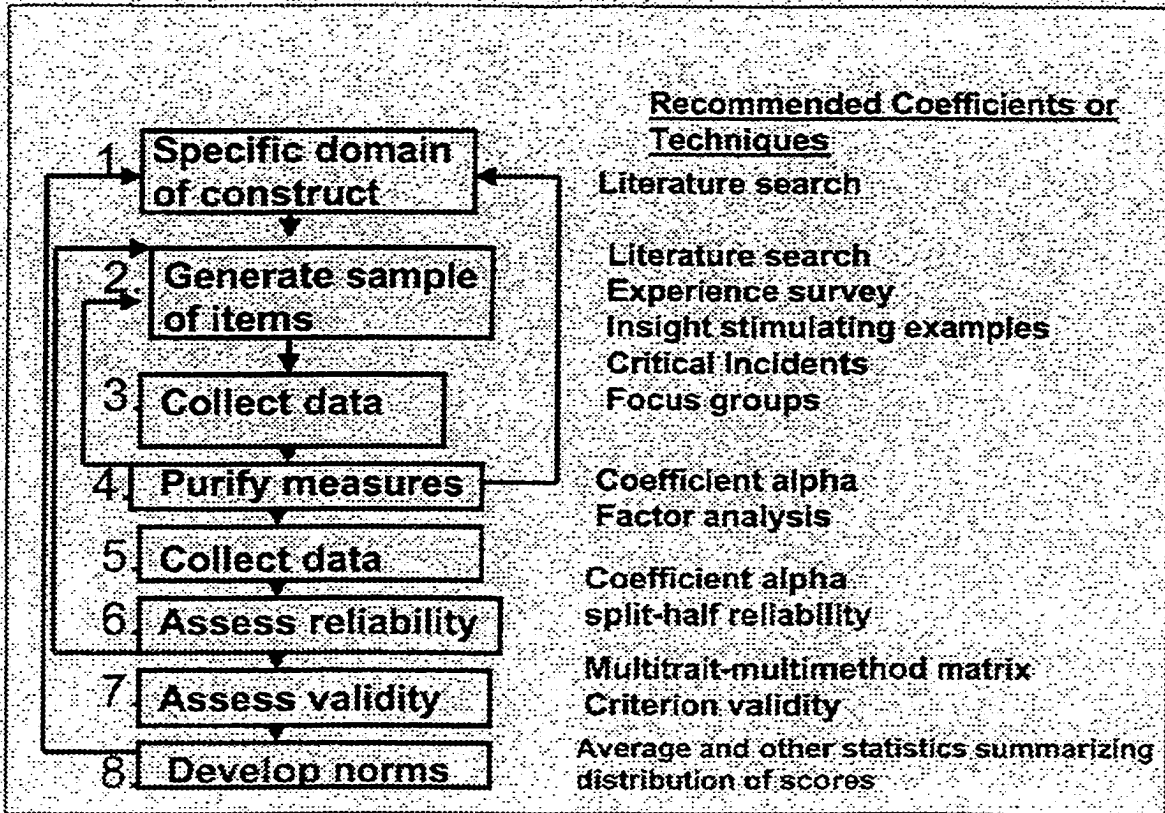


Figure 8. Suggested Procedure for Developing Better Measures.

Security, Audit and Control; Data Communication, Measurement and Evaluation, and Management Information Systems. This step was planned to insure a population of organizations with mature security risk management cultures and with different levels of business risk and organizational characteristics from which the sample was to be drawn. This selection method would place the sample of firms into the category of a purposive, nonprobability sample (Kramer & Dutton, 1991).

There are a series of steps associated with sample selection usually taken to control for firm autonomy (Child, 1973). The steps include a selection process to eliminate subsidiaries or divisions of other firms and corporate headquarters locations of organizations. This step is taken since the decisions made by firm level management relative to the realized strategy,

structure, controls and culture could have been influenced by a corporate level series of decisions. For this research study, this action step was not planned since leaving these sites in as part of the population would insure that corporate headquarters and parent firms' actions were accounted for. The realized firm level SRM strategies usually result from corporate level decisions. However, only an organization's primary business was to be used for analysis purposes. The firms that were diversified were to be evaluated as to the percentage of diversification and if the secondary business was more than 30% of the total sales, these firms were to be eliminated from the sample. This step was planned to insure that the firm management had focused on the primary industry level risks (business and security) that helped to shape the existing SRM program. The researcher made the decision based on an assumption that if more than 30% of total sales, came from a different industry, different TMT members would have to focus on different industry sectors to deal with the task environment risks in the different industry sectors (Daft, Sormunen & Parks, 1988). The number of firms that are left after this type of filtering process can have a major impact on the power of the statistical methods used for the empirical testing of the research hypotheses (Cohen, 1977). Therefore, every attempt was to be made to maximize the usable sample size available for analysis.

The Tomaskovic-Devey, Leiter and Thompson (1994) article on the theory of survey nonresponse influenced the original design of the original research strategy adopted for the dissertation research study. The package was developed to reflect their suggested methodology without unduly increasing the total cost of the unfunded research study or compromising the research strategy. Using this methodology should have helped to improve the overall organizational response rates for the research study and contribute to the overall usable sample size available for analysis and to the power of the statistical tests used.

The power of the statistical tests is determined by three factors: (1) the significance level, (2) the sample size, and (3) the effect size (Baroudi & Orlikowski, 1986). The

significance level is determined by what magnitude of Type I error the researcher will accept. Type I error measures the probability of rejecting a null hypothesis when it is true. Additionally, Type II error is the probability of failing to reject a null hypothesis when it is false. Beta is calculated as $(1 - \text{power})$. Cohen (1977), suggests that researchers should use a power = 0.8 for exploratory studies which will allow for 0.20 Type II errors, with a significance level of 0.05. The effect size is determined by the researcher based on what is suspected as to the degree the phenomenon being studied exists. It has been suggested that in exploratory research studies, the researcher should select a conservative estimate. For this study, the estimate used was to be (0.4), which would require different minimum usable sample sizes based on the type of data analysis and testing (i.e., T-test, F-test, and others). Additionally, the minimum sample size was to be evaluated relative to the potential for industry effects which could have created serious biases for statistically derived research results (Dess, Ireland & Hitt, 1990).

3.3 Research Instrument Development

The full eight-step Churchill (1979) research paradigm model is based on establishing the validity and reliability of measures. The model was to be followed for the development of the research constructs and their measures. The eight-step methodology includes a pretest phase that should result in a high level of construct validity. The methodology emphasizes multiple measures, interim analysis, factor analysis and feedback loops in the construct development process model (see figure 8). This should have insured a proper interpretation of the research findings for validity and the reliability of the research constructs based on sound psychometric principles (Venkatraman & Grant, 1986).

3.3.1 Reliability and Validity

The reliability of questions used to measure an underlying construct is an important consideration in research instrument construction. The reliability property is based on the

concept of measurement error and refers to the accuracy or the precision of measurement. Reliability is the degree of variation that occurs among scores on different measures that are due to random error, as opposed to systematic error. An absolutely reliable measure would have random error equal to zero. Therefore, measures that are more reliable will have less random error. When a large amount of variation exists between measures due to systematic error, then the assumption is that the measures are unreliable and therefore do not generate information that is consistent relative to the underlying construct. However, it must be understood that the property of reliability is a necessary but not sufficient condition for validity (Churchill, 1979).

A measure is valid when the true score is equal to the observed score on a measure of the construct. If the scores are in agreement then and only then can it be assumed that it only measures the construct in question. Therefore, the problem that is faced is to construct scales or measurement instruments that generate observed scores as close as possible to the true values. The Churchill paradigm is based on the truism that it is seldom know what the true value (score) is. Therefore, Churchill (1979) advocates the use of multiple measures since individual items have three major properties that reduce their value or validity.

First, individual items usually have considerable uniqueness or specificity in that each item tends to relate to other attributes as well. Second, single items tend to categorize people into a relatively small number of groups.... Third, individual items typically have considerable measurement error: they produce unreliable responses in the sense that the same scale position is unlikely to be checked in successive administrations of an instrument. (p. 66)

Since the research study used several measures that had not been validated, the full Churchill model was to be followed for those measures. One of the major goals of the dissertation study was to gain an understanding of the nature of the constructs and their relationships in the conceptual research model (Sethi & King, 1991). Therefore, the construct

validity of the instruments was an important issue for the study (Subramanian & Nilakanta, 1994).

3.3.2 Pilot Test Questionnaires

Two questionnaires were constructed for the pilot test phase of the research study. The first questionnaire was divided into two sections with one section that was to be administered to the highest-ranking security official (CSO) and the second section to the highest ranking IS official (CIO). The second questionnaire was to be administered to other high-ranking members of the TMT.

The research strategy used both multirespondents and single respondents from each firm. Where it was suspected that major differences exist between the CSO and other members of the firm management multirespondents were planned to be used. This is important for the questionnaire information measuring the SR knowledge and awareness of firm management, effectiveness of the SRM program, confirmation/disconfirmation, and desired performance of the SRM program. These were to be aggregated to develop a firm level measure for analysis.

Where it was planned to have multiple TMT respondents the goal was to attempt to have the CEO respond and at least one additional member of the TMT. It has been empirically demonstrated that different members of the TMT deal with business risks emanating from different sectors of the environment (Daft, Sormunen & Parks, 1988). Furthermore, different members of the TMT may perceive organizational outcomes differently (Bourgeois, 1985; McDade, 1990). However, if less than the entire TMT respond, and only the CEO response is received, that should be sufficient since CEOs perceptions have been shown to largely define the strategy of firms and also determine to a large extent the risk taking nature of the firm and also the risk management style of the firm (Hart, 1992).

The CSO was the single respondent for the section of the questionnaire containing the measures for the SRM Program, and the Actual Performance of SRM Program. The CIO was

the single respondent for the IT Resource Posture section of the same questionnaire. This step assures that the most knowledgeable respondent is would be the selected respondent and that the same respondent did not respond to questions related to a dependent and independent variable relationship.

3.3.3 Measures-Aggregation Error

The research study required combining subdimensions (aggregates) in order to be able to get indicators of broader constructs. Therefore, the possibility for aggregation error exists. The subdimensions of the research constructs have been identified from empirically derived evidence and in some cases solely on theoretical grounds or anecdotal evidence and practitioner experiences. Therefore, reliability assessment became a topic of major importance for the dissertation. Inadequate internal consistency amongst the subdimensions of the theoretically derived indicators of the broader constructs would imply that they are idiosyncratic to the items included in the instrument (Schwab, 1980). The use of Cronbach's Alpha was to be computed separately for each of the perceived composite scales to assess the overall reliability. The minimum suggested is 0.70 for minimum reliability (Nunnally, 1978, Nunnally & Bernstein, 1994). Additionally, the relationships between items and sets of items were to be examined in order to test the internal consistency of the composite scales used. The average item-total correlation's across the scales was to be used to check for the adequacy or reliability of the measures (Nunnally, 1978).

3.3.4 Single Informant

The research study used a single informant for several sections of the research instrument. Where the same informant or the same type of data collection technique is used for both the dependent and independent variables on a research instrument, this situation is classified as a form of common methods variance (Doty et al., 1993). There was an attempt made to avoid using the responses of a single respondent for both dependent and

independent variables. Since the anticipated response rate was expected to be extremely low (less than 20%) due to the length of the original two research instruments and the sensitivity of the topic being investigated, this condition was simply recognized.

3.3.5 Domain Specification of Constructs and Sample Items

A systematic review was made of the relevant literature in the fields that were thought necessary to establish the construct domain of the original research model (see figure 6). There were discussions held with colleagues, faculty committee members, and authors in the security field via e-mail. The Internet was used to find relevant sites that might hold information specifically relevant for establishing the domains of the constructs. This process led to the development of sample items that were operationalized and were included on the preliminary questionnaire. The sources came from a review of research in the fields of strategy, organization, diverse areas that have researched the concept of risk, limited IS security related research, the general IS security press, and from special interest electronic publications.

3.4 Construct Operationalization

The definitions used for the revised research model, used for the data collection phase of the research study (see figure 7), constructs and their dimensions are included in table 3. Additionally, the revised research model constructs, dimensions and measures are identified in table 4.

3.4.1 SRM Program

The SRM program construct is the most extensive in terms of the measures being used to capture the posture surrogate. The major informant was the highest-ranking security official who was asked to fill out an extensive questionnaire covering the known domain of the construct. The SRM Program construct was operationalized using the concept of Posture to capture different program configurations along a continuum. The four measures that were

used allowed a positioning along this dimension from hard < > soft. The measures were to be aggregated in order to position an individual posture on the hard soft continuum based on governance, countermeasures, structure, and policy and procedures.

The basis for the SRM program portion of the questionnaire was a research instrument used by Straub (1990). After a review of practitioner articles, empirical surveys, Internet sites and electronic journals, it was determined that modifications would be required to reflect current conditions. The following major sources were used to develop the questions on the preliminary questionnaire: Herold (1994), Plant (1993) and Wood (1995). The Herold article was the main source that provided content and process issues associated with what factors should be included in an SRM program that are considered important for successful information security programs. It was anticipated that the new questions would insure a high level of content validity and insure a solid “practitioner purge” of the SRM posture dimension.

3.4.2 IT Resource

The IT resource construct has been operationalized, using the concept of posture as the surrogate, to capture the broad selection of different IT configurations that organizations can incorporate. Three measures are used to position a firm along a continuum from narrow < > broad. The measures were planned to be aggregated to position an individual firm’s IT posture using measures of strategic integration, EI level, and reach and range. The questions that tap strategic integration have been adapted from Chan (1992). The nine questions selected were determined to be the most relevant due to their focus on internal and external integration. The questions do not include any overlap with the EI level or reach and range measures. In order to insure that the questions fully tap the domain of this construct, the CIO was the selected respondent. Similarly, the six questions used to measure EI level and the two questions used to measure reach and range were administered to the same respondent. The EI level is

assessed using six questions that use six-point scales from (too a large extant/not at all). The questions have been constructed to fully cover the EI level domain as identified by Venkatraman, 1994. The reach and range dimension uses the framework proposed by Keen (1991). The questions are adopted from Broadbent, Weill, O'Brien and Neo (1996).

3.4.3 Organization

The selection of the appropriate measures to measure the surrogate, organization posture, involved reviewing existing research studies in the business policy/strategy and organizational fields followed by interviews with management faculty at two southern universities. The use of existing validated research instruments for strategy, structure and task environment measures were obtained and reviewed. A major research premise was to use established prior validated instruments for use wherever possible in order to increase the validity of the research study results. The selected measures were used in prior research studies and specifically have been used for research studies related to an extensive series of research propositions and evaluations relative to the Miles and Snow typology (Doty et al., 1993). The instruments have multiple item scales and were used in conjunction with testing the suitability of the ideal type notion of the Miles and Snow typology. The measures exhibit a high level of validity and reliability. This aspect was important since a self-typing approach was used to identify strategic archetypes. Therefore, the dimensions of the strategic archetypes identified could be cross-validated using the structure responses. The terminology used in these instruments has been used across an extensive array of industries. Therefore, they were deemed to be acceptable to use across the industries that would be present in the research sample.

3.4.3.1 Decentralization

The dimension was selected to reflect the organizational distribution of power in the organization. The dimension captures the reverse of centralized decision-making where the governance of the organization is under the complete control of central authorities. This

dimension was to be used to aid in identifying any dysfunctional governance relationship within a SRM program. The eleven questions are from Miller, Droge and Toulouse (1988). They have shown a high level of validity and reliability in previous research studies.

3.4.3.2 Integration

The dimension was selected to reflect the organizational dependence on intended rationality in strategy making (Miller, 1987). This dimension captures the use of task forces and committees, which would be a counterpoint to reflect a potential high level of communication between the security organization and general management. The eight questions are from Miller, Droge and Toulouse (1988). They have shown a high level of validity and reliability in previous research studies.

3.4.3.3 Formalization

A useful way to describe an organization structure is to use one of the major ways that have been developed in organization and strategy research. Formalization, integration, and centralization have been identified as being among the most consistent (Miller et al., 1988). The dimension was operationalized using six control questions, five functional and five specialization questions to establish the general level of formalization present in the organization. The questions have been directly adopted from (Miller et al., 1988).

3.4.4 Contextual Factors

The selection of what factors were used as control variables involved reviewing existing research studies in the business policy/strategy and organizational fields followed by interviews with management faculty at two southern universities. The final selection process identified the most appropriate that should be used based on the proposed research questions. A major consideration was to use established prior validated instruments for use wherever possible in order to increase the validity of the research study results.

3.4.4.1 Size

The control variable has been a topic of organizational science interest since the earliest organizational studies were conducted. The seminal work on management organization conducted by Woodward (1965) is one of the early examples. Size has also been an important contextual variable in strategy, innovation adoption research, and MIS success (Damanpour, 1991; Ein-Dor & Segev, 1978; Doty et al., 1993). There have many different ways it has been measured based on the context of the research (i.e., number of employees, sales). The current research study measures size based on two dimensions that have been used as control variables in previous SRM program research studies (Goodhue & Straub, 1991). There are three questions related to number of employees/computer users and one multi-level question that measure the current level of the IT platform.

3.4.4.2 Strategic Archetypes

The Miles and Snow (1978) strategic archetype operationalization captures the strategic decision-making process patterns organizations have adopted. The Miles and Snow classification typology includes: Prospectors, Analyzers, Defenders, and Reactors. The use of this typology allows the researcher to capture three major issue areas the CEO and TMT must deal with: entrepreneurial (define and choose product-market domain), engineering (selection of technologies for the production and marketing processes) and administrative (rationalize existing organization structure with possible selection of new directions). The self-typing paragraphs developed by James and Hatten, (1995) in their research study of 399 banks were used. The self-typing paragraph approach to measure this construct has reported prior results, which suggest high reliability and good evidence for the convergent validity of this approach. The Miles and Snow (1978) typology has been defined as ideal types of unique configurations of contextual, structural, and strategic factors that include the equifinality assumption that there are multiple, equally effective organizational forms. Many past studies have also treated the

analyzer as a midpoint on the continuum from prospector to defender rather than as an ideal type. Additionally, the situation of treating the reactor as an ideal unique type or as a residual category for ineffective organizations has also occurred. The dissertation research study used the ideal type definition for all four configurations. This action was taken since some of the previously reported emergent organizational forms identified in chapter one may have characteristics similar to that of the reactor as identified in the Miles and Snow typology. Additionally, using the ideal type form could further aid in positioning a firm as a business risk taker or as a business risk avoider.

3.4.4.3 Structure

The control variable was operationalized using five questions to establish the level of organic structure present in an organization. The questions have been directly adopted from the “Organicity Scale” used by Covin and Slevin (1988, 1989). The questions were administered to the entire TMT and their answers were to be aggregated to establish a firm level measure of the collective management style of the organization. This was considered to be an important control due to the possible dysfunctional situation that could arise between a hard SRM posture and an organic organizational structure due to the mechanistic types of dimensions required for a hard SRM posture (Herold, 1994).

3.4.4.4 Industry

The control variable was measured using one, two part question. The variable was used to make a distinction between the primary and secondary industry sectors within which the firms operate. This was to be a device to screen firms for diversification by identifying firms with sales in more than one primary industry where the sales in the second industry exceed 30% of total sales. This was planned to avoid the problem of multiple task/multi-business organizations. This step was used to insure that the management had focused on the primary business and security risks in their primary industry. The sectors included on the questioners

were identified through reviews of existing information security surveys.

3.4.5 Firm Management Characteristics

The Firm Management Characteristics construct was operationalized using two multi-level dimensions. The measures were constructed to reflect the multidimensional nature of the construct. The SR knowledge and awareness dimension has a set of measures that use a triangulation methodology to capture the current knowledge and awareness of potential security and business risks associated with the deployment of the IT resource. The questions include potential new security risk areas selected from the reviewed practitioner press include in chapter one of the dissertation. The SR knowledge and awareness dimension uses twenty-seven questions. A qualitative risk evaluation methodology was incorporated to construct the multidimensional questions (Bennett & Kailay, 1992; Bodeau, 1992). Additionally, The results of the Holtgrave and Weber (1993) research study was used to incorporate the notion of relevant risk perception dimensions isolated by Slovic, Fischhoff, and Lichtenstein, (1977, 1986). The technique captures the essence of the severity or the business impact of a security breach and the likelihood of a security breach. The overall qualitative risk measure (level) is multidimensional. The severity factor is divided into four levels (Catastrophic, Critical, Marginal, and Negligible). The likelihood factor is divided into four ranges (highly possible, possible, unlikely, highly unlikely).

The Risk Propensity dimension was measured using five questions measuring business risk. The measures used to indirectly measure the business risk propensity of firm management was adopted from a research study that used firm business risk taking as one dimension of the strategic orientation of business enterprises (Venkatraman, 1989a).

3.4.6 Executive Management Support

The Executive Management Support construct was operationalized with two dimensions. The measures were constructed to reflect the multidimensional character of the

concept as developed by Jarvenpaa and Ives (1991). The construct is operationalized using measures of involvement and participation. The questions are adapted from the suggestions found in an awareness and involvement organizational assessment checklist (Fisher, 1984).

3.4.7 Actual Performance of SRM Program

The construct was operationalized using three dimensions that measure the residual net negative business consequences of the total number of security breaches and the severity level of the security breaches experienced by the organization, in the past twelve months. Originally, the objective measures, were adapted from Straub (1990), and they were updated using the Parker (1995) categorization scheme (see table 2). The modified measures were to measure a twelve-month period of performance rather than using the Straub three-year period of performance. A second set of questions was developed that are a perceptual qualitative set that capture the business impact of the security breaches experienced in the past twelve months relative to other firms in the same industry. The research plan included the option for the participants to only answer the perceptual set if they were reluctant to report actual figures.

3.4.8 Desired Performance of SRM Program

The construct was operationalized using the same dimensions as were used to operationalize the perceptual relative actual performance measures of the SRM program. The wording was modified to measure the desired residual net negative business consequences of the total number of security breaches expected by the organization during the past twelve months. The qualitative set of questions were to be the only ones administered since it did not seem realistic to attempt to measure quantitative desires.

3.4.9. Effectiveness of SRM Program

The construct was operationalized using two stand alone dimensions. The dimensions were developed based on an article by Seddon, 1997. In the article, the DeLone and McLean (1992) model of IS Success was clarified and it was suggested that success comes from the net benefits derived from using the system. The net benefits derived from the system are used as a surrogate measure of system effectiveness. The Seddon (1997) respecified model of the Delone and McLean (1992) model identify Perceived Usefulness and User Satisfaction as general perceptual measures of the Net Benefits of past IS use. In the dissertation research study, nine questions are used to measure perceived usefulness to reflect three major tradeoffs that must be considered when developing an effective “real world” SRM program (Wood, 1995). These include cost/security; flexibility/security; ease-of-use/security. Additionally, a separate stand alone measure of the effectiveness of SRM program was developed. The measure of perceived employee compliance was identified as being mandatory for successful SRM programs (Herold, 1994; Warman, 1993). The questions for this measure have been adapted from Straub (1990).

3.4.10 Confirmation/Disconfirmation

The construct was operationalized using the same two dimensions used to operationalize the actual performance and the desired performance of the SRM program. The gap measures the difference between the desired performance levels and the actual performance levels of the SRM program over the past twelve months. The level of disconfirmation indicates the degree to which perceived actual performance exceeds desired performance. The questions are based on a format and methodology adopted from Suh, Kim and Lee (1994). The methodology uses a five-point scale so that negative confirmation points are assigned with negative scores and positive disconfirmation with positive ones,

poorer than desired = -two; a little poorer than desired = -one; just as desired = zero; a little better than desired = +one; better than desired = +two.

3.5 Instrument Pre-test, Pilot test and Modification

The content validity for the instruments was established through several different procedures. In order to fully develop the domain of the constructs, a large representation of measures were generated to fully tap the constructs to insure a high level of content validity (Carmines & Zeller, 1979; Kerlinger, 1973). An extensive search of the practitioner press on security, academic journals in many different fields, and general management publications were reviewed for relevant material that was identified as related to the constructs and the measures used to indirectly measure them. The major premise behind content validity is to adequately sample the various regions of the universe of the construct by providing sufficient measures.

The separate sections in the preliminary questionnaires contained multiple questions for each measure. This action should insure that the domain of the constructs has been captured. The preliminary research instruments contained questions (response items) that were used to solicit respondent answers relative to the current domains. Several different scales were employed for different aspects of the operationalization.

The instruments were pretested using the methodology suggested by Chan and Huff (1994), on a convenient sample of Management and Management Information Systems faculty members at a south central university and at a northeastern university. In the Chan and Huff methodology, an instrument review was conducted by senior management at Manufacturing and Financial services organizations.

The faculty panels used for the dissertation study were asked to comment on the construct definition, the suitability of the operationalization (the dimensions) and the questions used to measure the dimensions. The responses were used to modify and refine the

instruments. The results of the pretest were used to develop the instruments for the next phase of the validation process. The plan was to pilot test the refined instrument with a sample of two firms, which have known mature security risk management cultures. A convenient local sample of firms was identified and five firms agreed to take part in the pilot test prior to seeing the pilot test questionnaires. The original plan was to first use two firms that were willing to cooperate via a field study. The five sites were carefully selected based on characteristics present in their current SRM program. The plan was to administer the preliminary questionnaires to willing members of the TMT and the CIO and CSO. The respondents were then to be given an opportunity to make comments on the constructs, relationships and construct dimensions during a series of semi-structured and structured interviews. The original plan included the possibility of tape-recording the conversations during the closed and open-ended interviews. The interviewed managers were going to be asked for permission prior to any recordings being made. The qualitative nature of the planned interviews should have aided the researcher to gain a richer understanding of the current security culture. The planned interviews were to focus on the dynamics of the research model and the constructs, dimensions and makeup of the questionnaires. The historical nature of the evolution of the existing security culture was also to be addressed. An essential input that was expected from the pilot was an evaluation by the participants as to the level of meaningfulness of the scales used for the questions. The responses were to be used to insure that the scales covered the entire range of the dimensions. However, the content validity of the instruments would not be tested since only judgmental decisions would be considered and in order to gain confidence some type of consensus is required (Cronbach, 1951; Cronbach & Meehl, 1971).

After the in-depth analysis of the data collected at the model firm sites, a decision was to be made as to the desirability of further field study at additional sites. The additional firms

were to be drawn from the convenient sample of five firms. The process steps are similar to a multi case methodology used by several organizational researchers. Examples include Eisenhardt (1991, 1989a) and Eisenhardt and Bourgeois (1988) who used a multi-case design in their studies of firms in the microcomputer industry. The methodology uses a replicative logic (Yin, 1989). Multiple cases are treated as a series of separate research experiments. The individual cases are used to confirm or disconfirm the inferences the researcher has extracted from all of the previous ones conducted. The studies use multiple data sources throughout the series of cases conducted. The Eisenhardt studies used CEO interviews, TMT semi-structured interviews, TMT questionnaires, and secondary archival data sources. The results of the research studies were used to develop mid-range theories.

The pilot test data was to be put through an extensive data screening and purification process following the recommended procedures as outlined by Tabachnick and Fidell (1989). A process was to be used to systematically verify that the measures would be useful for the purposes of the proposed research study. A combination of factor analysis and coefficient alpha was to be used for this operation. The researcher must caution against any interpretation of the labeling of components of a principal component factor analysis of the different risk characteristics that imputes or implies any type of psychologically associated reality with how the labels are constructed. Finally, the results of this process were to be two research instruments suitable to move on to the next phase of the Churchill model.

3.6 Data Collection

The purified instruments were to be mailed to the research sample of firms obtained from the membership listing of the ACM-SIG membership listings. The survey instruments were going to be mailed to the CEO and one member of the TMT of the research sample firms. Tomaskovic-Devey et al. (1994) identify high rates of nonresponse to organizational level surveys as creating the potential for large amounts of statistical biases in the final sample.

Therefore, in order to receive 100 usable survey responses a minimum of 500 surveys were to be mailed out in the first mailing. Kim and Mueller (1978) specify that a minimum sample size should be equal to 51 plus the number of variables that will be statistically tested. Nunnally (1978) suggests that the sample size should be at least four to five times the number of variables. The exact number of variables could not be determined until the finalized research instruments were available.

The data was to be collected from the sample and after the data screening and purification process was completed, the reliability of the instruments was to be established using coefficient alpha. The reliability was to be calculated for each of the scales. The use of a 0.70 value for Cronbach's Alpha was to be used to establish the cutoff value as suggested by Nunnally and Bernstein (1994). The scales that had a calculated reliability coefficient below 0.70 were to be discarded. The next step was to use factor analysis to determine the unidimensionality of the surviving scales. The methodology was going to be used to check items to see how they co-vary in order to see if they are measuring the same underlying construct. The potential exists for the absence of unidimensionality, which would indicate that the reliability coefficients could be biased. The content and construct validity of the instruments was going to be tested during the next step in this phase of the process. The methodology was going to follow the outline mentioned earlier in this chapter. The procedure suggested by Kerlinger (1973) using factor analysis and correlating item scores with total scores was going to be followed during the construct validity phase of the process.

Common Factor Analysis was to be the statistical technique utilized to reduce the large set of data collected into a smaller set in order to identify the dimensions of the measures. The expected result is that the measures that belong together will form factors. The measures that form a factor will be more highly correlated with each other than with measures not included in the same factor. The technique has come under criticism since

what has been established was identified by the researcher and does not exist on its own. The researcher must establish the presence of the factor via other means. Carmines and Zeller (1979) caution that anything responsible for creating correlations between variables will create factors. Secondly, the factors extracted from one data sample may differ in composition from sample to sample. Additionally, factor analysis can lead to misleading conclusions if interpreted without theoretical guidance during the construct validation process. Subramanian and Nilakanta (1994) have identified an additional series of considerations a researcher must be aware of when using principal component analysis or exploratory factor analysis for construct validation.

The next planned step was to be a methodology suggested by Nunnally and Bernstein (1994) to correlate individual items with total scores. The methodology is based on the premise that total scores are correct. The total score should have the individual item extracted in order to reduce spurious effects associated with the item. The individual items should then be correlated with the total score. A correlation of 0.30 is suggested as being sufficient to indicate construct validity. The use of multi-trait, multi-method matrixes is further suggested by Churchill as a further method for establishing validity. However, it was realized that steps would be too costly for an unfunded dissertation study.

3.7 Develop Norms

The final step in the Churchill methodology is to develop norms (i.e., means and standard deviations). The norms are the tools used to test research hypotheses based on the relationships established by the constructs. Additionally, there should be cross tabulation tables and frequencies generated from the demographic and descriptive portions of the research instruments.

The hypotheses were going to be tested with data collected from firms that survived the filtering process described earlier in the chapter. Finally, a series of multiple regression

models were to be developed to test the research hypotheses. Depending on the specific relations between different independent and dependant variables, various combinations of the control variables were going to be introduced into the regression models.

CHAPTER IV

REVISED RESEARCH STRATEGY AND RESPONSE RATES

4.0 Introduction

Chapter 4 is divided into major sections which include: the pilot test results, the resulting major research strategy changes that were required after the pilot test, and the response rates obtained from the data collection phase of the research study.

4.1 Pilot Test Results

Eighteen months after the preliminary research instruments were finalized; the pilot test stage was terminated after 42 of 43 organizations contacted refused to take part in the field study. Originally, five firms agreed to take part in the pilot study and it was anticipated that at least two would actually take part in the pilot study after they reviewed the preliminary research instruments. After reviewing the questionnaires all five declined to continue. The organizations were furnished a research study proposal and copies of the preliminary questionnaires. The organizations were told that the self report questionnaires should be given to the designated managers and that follow-up interviews would be required to improve the relevance, clarity and content of the questions. Additionally, the interviews would also be used to gather suggestions that might be used to improve the quality of the finalized questionnaires. The organizations were told that they would receive an executive review profiling their firm so they could make useful comparisons with firms in the same industry after the research study was completed. Finally, they were told that nothing that would reveal organization identity or individuals in the firm would appear in the published results of the study. After the rejection by the original five firms a series of methods were used that isolated 38 suitable organizations that were contacted to find out if they would take part in the pilot study. The methods used included colleague

and insider referrals and introductions, contacting professional organizations that had either sponsored, supported or published information security surveys, contacting leading security industry firms, contacting consulting firms that have a visible presence in information security, contacting several governmental organizations and making a presentation at a USENIX security symposium in order to solicit support. These activities resulted in a series of meetings with IS and security personnel at several firms, and a presentation made via teleconferencing to high level managers at several locations of a government agency. The net result of this activity was that one firm agreed to participate, responded to the questionnaires and allowed the necessary interviews to take place. The reasons given by the 42 firm representatives that refused to have their firms take part in the pilot test phase of the research study have been summarized and are shown in table 5. As reported, 35.7 % would not take part due to efforts required to deal with the Y2K problem; 11.9% were concerned that top management might become too interested in the firm information security programs and make requests about what was being done in this area. Many were concerned that this type of research study might lead to problems for them individually at their firm and potentially held major negative consequences for them.

The firm that took part in the pilot study is a leading firm in the security industry. In order for them to participate an agreement had to be made that an employee of the firm must conduct the interviews and that the researcher had to agree to not reveal the company identity. The director of Educational Services conducted the interviews and he proved to be a valuable contact. The educational services director—Ph.D. in statistics—has conducted research studies in Information Security Policy and Social Psychology. The participation of this firm proved extremely beneficial in developing the finalized research instruments. The CIO, CSO, two TMT members, and a second CSO/CIO questionnaire answered by the director of education all provided insightful information about the content and structure of the research instruments.

4.2 Research Instrument Modifications

The original research strategy included the use of two self report research instruments that would be mailed to each firm. The first questionnaire contained sections that were to be answered by the CSO and several additional sections for the CIO. The second questionnaire was to be distributed to several different members of the TMT. The original goal was to obtain a minimum of 100 usable firm survey responses from an initial mailing to 500 firms. The limited response rate experienced during the pilot test raised concerns that to obtain 100 usable survey responses would require a minimum mailing to 4,300 firms. Eliminating the reported Y2K issue from consideration reduced the target number of original mailings to 2,800 firms. This was based on an estimated response rate of 3.6%. This target was based on a Kim and Mueller (1978) specification that a minimum sample size should be equal to 51 plus the number of variables that would be statistically tested. Additionally, Nunnally (1978) suggested that the sample size should be at least four to five times the number of variables. The costs associated with the logistics required for such an effort were totally beyond the limited budget of the research study. Finally, the structure of the questionnaires was modified so that only receiving the CSO questionnaire and one of the other three would still allow testing hypotheses associated with portions of the revised research model (see figure 7). This action would require fewer than 100 usable CSO and one of the other firm member responses. The target response goal was set at between 75 and 100 usable firm level survey responses. The elimination of the firm refusals from the pilot study for job security issues (6) and for required top management explanations (5) meant that this revised required response rate of 6.3% would require an original mailing of between 1,200 and 1,600 to provide between 75 and 100 usable firm responses.

The feedback obtained from the pilot test firm participants and intelligence extracted from the reasons given by the 42 firms that refused to take part led to the following

modifications being made to the content and structure of the research instruments. The original two questionnaires were divided into four questionnaires that would be responded to by the CIO, CSO, a member of the TMT and a functional level manager. This action was taken in order to reduce the time required for each participant to complete the questionnaire and to insure that any other firm member would not see the CIO and CSO answers. In order to further reduce the potential response time all questions used to measure the SR Knowledge and Awareness of firm management were eliminated. Additionally, all questions that required quantitative information for the Actual Performance of the SRM program and all of the questions that required quantitative or qualitative answers for the Desired Performance of the SRM Program were eliminated. The pilot test firm identified these areas as the most intrusive aspects of the research study and the researcher determined that eliminating them should help to improve the expected response rate. Finally, the wording of questions in several sections of the research instruments was modified to increase their clarity. In order to increase the potential survey response rate it was determined that a maximum target time should be 20 minutes for the CIO, TMT, and functional manager to fill out the questionnaires. The scope of the CSO questionnaire was the most extensive and the goal was to reduce the maximum time required to answer it to thirty minutes. The focus of the entire process was to eliminate as many sections of the questionnaire as practical and eliminate the sections that were considered highly intrusive or were totally original measures that would require the complete Churchill pretest process to validate (see appendix A). Additionally, it was determined that the sponsorship of an established university research center was an important factor to consider in order to improve the response rate. It has been suggested that a sponsor's name should be prominently displayed on the cover page of every questionnaire to enhance the professional appearance of the research instruments and to help establish the credibility of the researcher (Dillman, 2000).

4.3 Sample Selection Modification

The research strategy required a selection process that provided a heterogeneous industry population of U.S. firms in order to gain the maximum level of population generalizability while maintaining an acceptable level of precision in control and measurement of the variables (McGrath, 1982).

The original sample of firms was to be drawn from the membership listings of selected ACM-SI groups. The groups selected were to include the following: Security, Audit and Control, Data Communication, Measurement and Evaluation, and Management Information Systems. This approach was chosen in order to provide an adequate population of organizations with mature security risk management cultures and with different levels of business risk and organizational characteristics.

Feedback gained from conversations during the pilot test phase of the research study led the researcher to believe that firm size should be a major selection factor to tap a population of organizations with an established security risk management program. The discussions indicated that larger organizations, more than 500 employees, could afford the costs associated with formal information security programs and they also would be the most likely to have assigned security and/or risk management personnel. A mailing list broker was contacted that deals in specialized mailing lists and a database containing the names of CEOs and COOs of 5,001 U.S. business organizations was obtained that only included firms that employed more than 500 employees. A cross section of 1,500 firms was selected based on their primary SIC classification and employee size. Additionally, the attendance list from a recent major security symposium and conference was used to include companies if they appeared in the database.

4.4 Cover Letters

The original cover letter used during the pilot test stage was designed based on the Tomaskovic-Devey, Leiter and Thompson (1994) article on the theory of survey nonresponse.

The article influenced the design of the entire pilot test package and the original survey mail and follow-up strategy adopted for the research study. The cover letter for the data collection phase evolved along with all items that were planned for the data collection phase of the research study. The knowledge extracted from the intelligence gained from the pilot test cycle and the added information provided in Dillman (2000, 1978), reinforced the notion that rewards, costs and trust must be considered in every aspect of the package design. The cover letter should contain information that addresses specific concerns that company representatives might have about the trustworthiness of the researcher, about the specific time, and out-of-pocket costs the organization would be expending up front. They also wanted to be apprised of the rewards the firm would receive, both immediately and later, after the firm fully took part in the study (see appendix B).

4.4 Token of Appreciation

The notion of social exchange as explained by Dillman, 2000 and used in the evolution from the total design method (Dillman, 1978) to the tailored design method (Dillman, 2000) places heavy emphasis on the importance of rewards, costs and trust in the design and development of the mail survey research package. The suggestions extracted from both the tailored design method and the total design method indicate that giving a token incentive is effective in increasing the potential response rate all other factors held constant. Several alternative types of token incentives were investigated for inclusion in the package that would be sent to the 1,500 firms. This researcher had been involved in a mail survey research study that included a specific state flag pin as a token in order to enhance the response rate through instilling an unfulfilled obligation on the part of the recipients of the flag pins. The use of a state flag pin was ruled out due to the national scope of the present research study and the opinion that something unique would have to be developed that would reinforce the nature and importance of the research study topic. Additionally, that the token would have to be something

that the recipients would know that only a select few people in the United States would have the opportunity of obtaining regardless of whom they are. A series of vendors were identified that manufacture customized items that are easily obtained and that are sold with volume discounts. The decision was made to include a customized refrigerator type magnet as the token of appreciation. The token would have to identify the overall theme of the research study. The final choice was to have the slogan "Practice Safe Computing" printed on a business card size magnet. Several font types in different colors were tested on undergraduate students, faculty members and colleagues in order to select the combination that would be the final choice. These actions resulted in a selection of two fonts and two colors that were found to be the most appealing combinations by the individuals surveyed. Finally, 8,000 magnets were ordered for the mail survey packages.

4.5 Response Rate

The revised questionnaires were included in 1,500 survey packages sent out in three waves of 500 each. The package contained a cover letter addressed to the CEO or COO of the firm, four questionnaires, five tokens of appreciation and four self-addressed return envelopes. The extra token of appreciation was included to overcome possible resistance by the firm gatekeeper for the CEO in order to gain entry into the firm. The original research strategy called for the research instruments to be mailed to the CSO/CIO. Again, reviewing the results of the pilot test led to the conclusion that the research study required the CEO or COO to direct other members of the organization to take part in the study. The packages were sent out using preprinted addressed envelopes so that presorted first class postage could be obtained. This action was taken to minimize the postage cost without delaying the delivery time and to enhance the professional appearance of the research study by using envelopes that had a college logo and return address prominently displayed.

After each wave there were a significant number of return to sender packages from the U.S. Postal Service. The major reasons included returned mail due to firm forwarding permits expiring or and the CEO or COO leaving the company. A major effort was made to resolve what the new address was for the firm and the name of the new CEO or COO. An online business resource database was used and also web searches using several different web search engines to locate the company or the name of the new CEO or COO. The results of this activity were mixed and in many cases new packages sent out also were returned for the same reasons as the original packages. The decision was made that the time expended versus the results did not warrant any additional attempts in sending out further second or third packages to firms that had the first package returned. Based on the number of returns from the first wave of 500 the decision was made that additional firms would be selected from the mailing list database to cover the number of returns that probably would be experienced from the second and third batches sent out. Follow-up letters were sent out to firms that did not return at least one questionnaire within four-to-six weeks after the initial package was sent out (see appendix B). The letter contained an increased appeal for their participation and offered an executive summary report profiling the firm if all four questionnaires were returned. The letter in the original package offered a summary of the results if the firm returned the four completed questionnaires. A different follow-up letter was sent out to firms two-to-four weeks after they returned at least one questionnaire (see appendix B). This package contained supplemental questionnaires to replace the ones that had not been returned with additional postage paid return envelopes. A similar paragraph, mentioned above, was added offering the increased incentive to return the four questionnaires. The results of this activity produced an unacceptable number of responses required for any statistically meaningful parametric or nonparametric tests to be conducted.

The number of original complete research packages that were sent out was 1,540. There were 66 returned for the various reasons mentioned earlier that could not be resolved. The potential number of firms that could have responded was 1,474. The total number of firms that returned at least one of the four questionnaires was 23. This represents an overall firm response rate of 1.6%. The total number of questionnaires returned was 67 broken down as follows: 18 CSO; 18 CIO; 16 TMT and 15 functional managers. Additionally, nine firms returned four questionnaires, four firms returned three questionnaires, nine firms returned two questionnaires and one firm returned one questionnaire. The nine firms that submitted the four questionnaires represent a firm response rate of 0.61%. Finally, 13 firms returned the CSO and CIO questionnaires; 12 firms returned the CSO and TMT questionnaires; 12 firms returned the CSO and functional manager questionnaires; 13 firms returned the CIO and functional manager questionnaires; 13 firms returned the CIO and TMT questionnaires; 11 firms returned the TMT and functional manager questionnaires. The response rates are summarized by employee size in table 6.

4.6 Time to Complete Questionnaires

The times recorded on the returned questionnaires confirmed that the modifications made to the pilot research instruments resulted in dramatically reduced times required to complete the survey instruments. The average time for completing the surveys were as follows: TMT 9.5 minutes; functional manager 9.9 minutes, CIO 14.0 minutes, and the CSO 24.1 minutes. The projected times quoted in the cover letter was 10–20 minutes for the CIO, TMT and functional manager. The revised CSO questionnaire quoted time for completing the questionnaire was 20–30 minutes.

4.7 Non-Responses

During the data collection cycle there were several telephone conversations with CIOs, CSOs and risk managers about the goals of the research study, the makeup of the

questionnaires and what credentials were held by the researcher. Additionally, similar types of interchanges took place via e-mail. Based on early exchanges from the first 500 firm mailing, a decision was made to attempt to find out the specific reason(s) a firm did not take part in the research study. Dillman (2000) lists several reasons why individuals and organizations do not respond to mail survey questionnaires. The ones deemed applicable to the current research study plus the information extracted from the pilot study and the early exchanges during the data collection activity were used to develop a 17-item questionnaire (see appendix A). The questionnaire was included in the package sent out to the firms that did not return at least one questionnaire and also to the firms that did not return the supplemental questionnaires. This was done in order to maximize the utility value of the postage costs associated with the additional follow-up mailings. There were 74 firms that informed the researcher why they did not take part in the research study (see table 7). Interestingly, 47.3% of the firms went out of their way, identifying the firm on the non-response reason questionnaire. Several sources have suggested that firm identification is a major reason firms do not take part in mail survey research studies (Dillman, 2000). The responses were gathered via e-mail, telephone conversations and through the return of the 17-item questionnaire sent out to approximately 1,400 of the 1,452 firms that did not respond to the original research package. This represents a response rate of approximately 5.1%. Table 6 breaks down the response rate by firm employee size.

CHAPTER V

ANALYSIS AND INTERPRETATION

5.0 Introduction

Chapter 5 is divided into major sections that include the firm levels results, individual respondent descriptive statistics, and an evaluation of selected firm level results.

5.1 Firm Connectivity Characteristics

The firms that responded to the survey reported a high level of internal and external connectivity. The majority of firms had an IT platform that included networked minis and micros (88.9%), a WAN (83.3%); an intranet (61.1%), and an extranet (22.4%). Many of the firms allowed external entities to access the information resources of the firm. The percentage of firms sharing information resources with outside entities varied across the categories as follows: seven (38.9%) allowed customers; six (33.3%) allowed suppliers; eight (44.4%) allowed firms that were not customers or suppliers to access their information resources. Finally, three (16.7%) allowed all three categories to access their information resources. The employees at the firm locations surveyed were high level computer users. The reported computer user levels were at least 80% at 61.1% of the locations. Only at 11.1% were less than 30% of the employees computer users.

The level of reported installed intranets by the participants in this research study was high relative to a survey taken in 1996 by Forrester Research. The survey identified 16% of 50 large corporations as having an intranet (Cortese, 1996). The firms with intranets are vulnerable to insiders' gaining access to unauthorized proprietary organization data. These firms are being advised to install internal firewalls to deter potential intranet security breaches. This is important since there are estimates that 80% of all information security losses result from

company insider security breaches (Violino, 1996c). A recently released report by International Data Corporation indicates there were 30 million intranet users in U.S. organizations in 1999 and that reduced technology costs should allow connecting more users of intranets (Bruno, 1999).

The firms with an extranet share a major security vulnerability issue associated with electronic relationships with external entities. They all must deal with shared security responsibilities with extranet partners that require a high level of "trust." The highest level of external electronic integration involving knowledge base sharing carries with it the highest levels of required security measures. It is suggested that companies use virtual private networks (VPNs) to provide basic extranet security (Blough, 1999). The combination of deployed extranets and intranets places the organizations that took part in this research study in the position of being in a category of firms that deploy what has been called a Business Critical Intranet (BCI). This is highly vulnerable due to the organizations' placing themselves in a complex task environment laden with threats (Zona Research, Inc., 1999).

5.2 Firm IT Resource Postures

The firms that responded to the survey reported a high level of strategic integration (see table 8), high levels of electronic integration (see table 9) and levels of reach (see table 10) and range (see table 11) that are required to support the earlier reported levels of connectivity.

Specifically, the firms that reported high levels of strategic integration (SI) (Chan, 1992), high levels of electronic integration (EI) (Venkatraman, 1994), and high levels of both reach and range (Keen, 1991) are highly dependent on their broad IT postures to support their overall business strategies (Porter & Millar, 1995). This dependency is an indicator that they are highly vulnerable to both internal and external information security threats since their IT resource is integrated throughout their value chain and they have developed large numbers of relationships with external entities that must depend to a large extent on trust. These are characteristics of a

class of firms that are utilizing their IT platforms for both efficiency improvements and effectiveness enhancements (Robey & Sahay, 1996).

Relative to the overall SI mean = 3.846, 22.2% reported much higher SI levels mean <3.0. These levels generate higher levels of security risk due to the potential business losses associated with security breaches that would be more damaging for firms that exhibit a high dependency on the firm knowledge base for the business strategy of the firm (Tapscott & Caston, 1993). Additionally, 11.2% reported low levels of SI, mean >5.0. Overall, the firms reported a high dependency on their IT resource for directing and controlling their production mean=1.944 and using their IT resource to make improvements in their products and services mean=2.278. Finally, the firms exhibited a realization that controlling their knowledge base was a major factor for their long-term survivability mean=2.722 (Daft & Lewin, 1993; Davidson, 1993). This last condition may be a major factor in their decisions to deploy a BCI (Zona Research, Inc., 1999).

The firms reported overall levels of EI between 2.83 and 7.00. The distribution was as follows: 5.6% reported a mean EI level in the 2–3 range; 33.3% in the 3–4 range; 16.7% in the 4–5 range; 27.8% in the 5–6 range; 11.1% in the 6–7 range. The overall aggregated firm level was mean = 4.865. One firm reported an EI level of 7.00. The lower the number the higher the level of EI which are reflective of higher levels of potential security risks due to the elevated levels of potential security breaches to internal systems and information via direct connection to outside entities. These relationships depend on a high level of trust with outside entities and at the highest level of EI; the firm knowledge base becomes vulnerable to security breaches (Sherer, 1995). This situation potentially would be more damaging for firms that have a higher dependency on the firm knowledge base for the business strategy of the firm (Rangan, 1992). Additionally, the firms reported the highest levels of EI with their suppliers in order to check inventory status or initiate a release build transaction with their suppliers mean=3.889 and to

exchange information with their customers/distributors mean=3.944. Finally, the firms reported the lowest levels of electronic integration relative to sharing process information with outside entities mean=5.333 and sharing knowledge base information with outside entities mean=5.222.

The 18 firms that responded to this portion of the survey reported levels of reach and range that are realistic given the reported high levels of strategic integration and high levels of electronic integration required to support a broad IT Resource Posture position. The highest level of reach was reported by 50% of the firms. Additionally, 72.2% reported their range included the highest level possible. Again, this condition is reflective of the high levels of reported connectivity.

5.3 Firm Strategic Archetypes

The 16 firms that responded to this portion of the survey identified themselves indirectly as high business risk takers (Miles & Snow, 1978). Three firms 18.8% classified themselves as prospectors, eight firms 50% analyzers, and five firms 31.2% defenders. None of the firms classified themselves as reactors. Prior research results suggest that an organization is reluctant to classify themselves as a reactor which carries with it negative connotations (Covin & Slevan, 1988). Therefore, not having any firm identify themselves as a reactor is not unusual. In terms of a strategic risk taking continuum, reactors would be ranked at the lowest levels with prospectors being assumed to be at the high end followed by analyzers and defenders.

5.4 Business Risk Propensity

The 23 firms that had at least 1 of the 3 possible respondents answered this portion of the survey indicating that generally, they consider their internal actions more conservative relative to a willingness to allocate resources, choose markets and products in uncertain environments, and the overall level of decision making in the firm (Venkatraman, 1989a). Table 12 lists the five firm level business risk questions with the reported firm level aggregated response means.

Summarizing the five questions at the firm level revealed that overall the firms tend to be more conservative than aggressive in their internal major decision making activities. The overall firm level mean was 23.725. The firm level range was between 17.000 and 32.000. An overall aggregated score of five would indicate a firm level high risk taking style of decision making. The highest summarized score of thirty-five would indicate an extremely conservative style of decision making where the firm management are risk avoiders and are not willing to experience a high level of business risk relative to allocating company resources (Lamkin & Courtney, 1995). Three firms (13.0%) had aggregated scores <20, 12 firms (52.2%) had aggregated scores <23.725, eight firms (34.8%) had aggregated scores between 24.0 and 27.00, and three firms (13.0%) had aggregated scores >27.00.

5.5 Structure

The 15 firms that responded to this portion of the survey indicated that generally, they have firm organization structures that are more mechanistic rather than organic in terms of formalization controls, job descriptions, and management principals that have worked in the past (Miller, Drouge & Toulouse, 1988). However, they also indicated that individual managers are allowed individual flexibility to deal with existing conditions (Daft & Weick, 1984). Table 13 lists the five firm level structure questions with the reported firm level means. Summarizing the five questions at the firm level revealed that five firms (33.3%) considered themselves more informal and flexible letting conditions dictate what has to be done in order to accomplish management activities aggregate mean >4.00. The highest firm aggregated score was mean=4.60 and the lowest was mean=2.40.

5.6 Executive Management Support

The 18 firms that responded to this portion of the survey identified several different individuals to be the active sponsor for information security interests. Six (33.3%) of the firms identified more than one individual as the active sponsor for information security. The

CIO was identified by five (27.7%) of the firms as one of the major sponsors. Additionally, the CEO/President, CFO/Controller and the MIS director were identified by four firms (22.2%) as one of the major sponsors. In two (11.1%) of the firms the Information Security officer or someone at the VP level was the major sponsor for information security interests. One firm (5.6%) indicated that its corporate security director was one of the major sponsors with the CEO/President of the company.

Table 14 lists the five executive involvement questions with the reported firm level means. The amount of executive involvement was high— <4.0 in 12 (66.7%) of the firms. However, this left six (33.3%) of the firms where executive support was $=$ or >4 overall. The area that led all areas in limited executive support was for a comprehensive information security education and training program. Six (33.3%) of the firms recorded a five or higher on this area. The area that had the highest levels of executive involvement was in the area of supporting the establishment of plans, policies, programs, and guidelines for information security. Eleven (61.1%) reported a two or one on this question. This seems to be consistent with research studies associated with IT projects where management will support a new initiative and then not fully support the training and education programs with the budgets required to qualify end users to use the new system (Dalton, 1998).

Table 15 lists the five firm level executive participation questions with the reported firm level means. The amount of overall executive participation was lower than reported executive involvement. Here, eight firms (50%) reported <4.0 and eight firms reported executive participation $=$ or >4 overall. The area that led all areas with the lowest levels of executive participation was the development and implementation of security controls. Eight (50.0%) of the firms recorded a five or higher on this area. The area that had the highest levels of executive participation was the understanding exhibited by general management about the terminology and requirements of information security in the organization. Six

(33.3%) reported a two or one on this question. The responses seem to be consistent with research studies that suggest that top management does not take an active participation role unless things are not going well.

5.7 Security Risk Management Program

This area is the most extensive in terms of the questions used to identify the dimensions of a firm level security risk management program. The 18 firms that responded to this section of the research study reported a wide variety of program characteristics. A majority of the firms (72.2%) has a published firm level security policy; and 66.7% have updated the policy within the past 12 months. Three of the firms did not know if they ever updated the security policy.

Table 16 identifies how the current security policy was developed and what type of management support was applied prior to it being issued. The area that had the highest level of prior support was receiving inputs from many members of the organization. Seven (38.8%) of the firms recorded a two or one on this question. The area that had the lowest level of up front support was in the budgeting activity required to keep the program up to date. Only three (16.7%) firms recorded a two or one on this question. Overall seven (38.8%) of the firms scored an overall mean of three or less as an aggregated mean score on the three questions.

Table 17 identifies the characteristics of the current security policy process at the 18 firms that responded to this section of the survey. The organizations reported a high level of usage of suggested techniques that should be practiced in their security policy process (see table 2). Eight (44.4%) of the firms reported a two or one on using risk management or audit techniques to identify threats and vulnerabilities and used audit reviews to monitor risk levels. The least used technique that the organizations use is penetration teams using social engineering to test information security countermeasures. Seven (38.8%) of the firms

reported a six or seven for this technique. Additionally seven (38.8%) of the firms had an overall aggregated mean score of three or less on the 10 questions.

The firms reported that a significant number (83.3%) have a designated spokesperson for making public announcements related to information security. Additionally, seven (38.9%) of the firms have quick reaction teams in place that are activated when a security crisis is experienced. Table 18 identifies the areas where the firms reported they have developed security plans that address the seven major areas that are usually mentioned that should be addressed in security literature. The least reported area covered in firm security plans was communication security where only seven (38.8%) addressed this area and one of the 18 firms reported that they did not have a security protection plan for the organization.

The firms reported a high level of both internal and external liaison relationships associated with information security matters. Internally, 10 firms (55.6%) had liaison relations between the information security organization and the human resources function and with facility management functions. Externally, five firms (27.8%) had a liaison relationship with their insurance companies and four firms (22.2%) reported that they had a liaison relationship with some law enforcement agency.

5.8 Security Organization

The 18 firms that responded to this section of the survey identified themselves as more centralized in their organization activities than decentralized. The mean score recorded on the three questions for 13 (72.2%) of the firms was 4. The range was from 1.667 to 5.000 on the 7-point scale from 1—very centralized to 7—very decentralized. Additionally, they reported that the primary responsibility for information security was at high levels in the organization. There were eleven (61.1%) organizations where the responsibility for information security resided at the VP level or higher. One firm identified the CEO/president as the person with the primary responsibility for information security. These

findings tend to support prior research results that indicate that having the highest level manager as a member of the TMT is an important factor for successful organization programs (Ein-Dor & Segev, 1978).

The highest level of centralization reported was relative to the purchase and deployment of security hardware and software. There were 10 (55.5%) of the firms that recorded a one or two for this activity on a scale of 1–very centralized to 7–very decentralized. The least centralized activity was in administering training, security awareness training, and conducting audits. There were six (33.3%) of the firms that recorded a four or five for this activity. The personnel who carried out security policy related activities were slightly less centralized than security hardware and software activities. For this activity, seven (38.8%) of the firms recorded a one or two for this activity.

5.9 Security Awareness

The 18 firms that responded to this section of the research study reported that eleven (61.1%) had security awareness programs and that seven (38.9%) of the firms had established goals for their security awareness programs. Additionally that five (27.8%) of these firms had employee security hotlines so that employees could report suspected security breaches without being identified.

The firms reported overall low levels of employee accountability for information security and low levels of training activities associated with the security awareness program. Table 19 lists the eight questions and the recorded mean scores. The 18 firms reported overall levels of employee accountability between 2.22 and 7.00. The distribution was as follows: 16.6% reported a mean in the two range, 11.1% in the three range, 5.6% in the four range, and 66.7% reported in the five-to-seven range. The category with the lowest support for employee accountability was the use of established rewards and recommended penalties for security compliance. The mean score for all firms on this question was 5.833.

Additionally, the firms reported overall mean scores on training between 2.33 and 7.00. The distribution was as follows: 11.1% reported a mean in the two range, 33.3% in the three range, 11.1% in the four range, and 50.0% reported in the five-to-seven range. The category with the lowest level of reported support was to solicit and use feedback from employees to make improvements in the existing program. The mean score for all firms on this question was 5.3889.

5.10 Security Risk Management Program Performance

The 18 firms that answered this section of the survey reported that the security risk management program they have in place has performed significantly better than what is expected in their industries relative to the number of security breaches experienced in the past 12 months. On a five-point scale from 1—extremely low to 5—extremely high. All firms reported a score of one or two on this question. However, two firms reported that the number of serious security breaches they experienced would be considered high or extremely high relative to their industry. Additionally, six firms reported that the number of nuisance types of security breaches would be considered average or above average relative to their industry. Seventeen firms reported that the cost associated with the security breaches they experienced in the last 12 months would be considered extremely low-to-low relative to their industry. Only one firm reported that costs associated with security breaches would be considered average for their industry.

The firms were asked to furnish information identifying how they detected security breaches and if more than one method was used to detect security breaches to put them in rank order of importance. Seventeen firms answered this section of the survey and identified a wide distribution of primary and secondary methods they used to detect security breaches. Five firms (29.4%) weren't sure what primary means were used to discover the security breaches. Four (23.5%) firms ranked normal system controls as the primary source of

discovery. Two firms (11.8%) ranked an employee reported observing a suspected security breach as the primary source of discovery and two firms (11.8%) reported that an employee discovered it by accident. Only one firm (5.8%) used security audits as the primary method used to discover a security breach. Additionally, two firms (11.8%) used a security investigation other than an audit as the primary method used to discover a security breach. Overall, regardless of rank order of importance the leading discovery means used were "not sure," six firms; "an employee who observed or suspected a security breach," five firms; "normal system controls," five firms, "by accident," five firms; and "through a security investigation other than an audit," four firms. These results tend to support some of the results obtained by Lim and Jamieson (1995) in their survey of 250 organizations. The firms reported a heavy reliance on existing controls to detect security breaches rather than considering using security audits.

5.11 Security Risk Management Program Effectiveness

Responses were received from 21 firms where either the CSO or a functional manager answered this section of the survey. At 12 firms, both the CSO and a functional manager answered this section of the survey. Responses were received from 15 firms where only a functional manager answered this section of the survey and from 18 firms where only the CSO responded to this section of the survey. Table 20 lists the 14 questions and the mean score responses for the firm level, CSO, functional manager responses used at firm level and the unique function manager questions. The survey contained three unique questions to generate a separate effectiveness measure to determine if there were differences using an independent effectiveness measure. The firm level means ranged from a high value of 3.917 to a low of 2.875. The highest firm level mean was for the understanding that end users have about security policies. At seven firms (58.3%), the firm level mean exceeded the total firm level mean for this question. The questions that recorded the most firm level means

exceeding the total firm level mean were for functional manager and end user adherence to the security policy where eight firms' (66.7%) firm level means exceeded the total firm level means for these questions. Close behind were the number of firm means that exceeded the total firm level means for the questions about the understanding that end users and functional managers have about the security policy. The total firm level mean for these compliance questions was exceeded by seven (58.3%) firms. The usefulness questions firm level means do not exhibit the same levels of exceeding the total firm level means. Only one question had more than 50% of the individual firm means exceeding the total means. The question related to internal operations that rely on accurate and timely data and information not being negatively impacted by security measures had seven (58.3%) firm level means exceed the total firm level means.

5.12 Confirmation/Disconfirmation

Responses were received from 20 firms where either the CSO or a member of the TMT answered this section of the survey. At 13 firms, both the CSO and a member of the TMT answered this section of the survey. Responses were received from 16 firms where only a member of the TMT answered this section of the survey and from 17 firms where only the CSO responded to this section of the survey. Table 21 lists the distribution of responses by firm, TMT and CSO. Reviewing the distribution of responses indicates that there seems to be a major split between the desired expectation performance and the actual performance level of the SRM program held by CSO respondents and a member of the TMT. The CSO differences about the number of security breaches experienced shows that 41.2% indicated that the number of security breaches was less than expectations. The TMT members responses about the number of security breaches experienced shows that 31.2% indicated that the number of security breaches was less than expectations. The split also exists for the estimated value of lost business where 52.9% of CSO respondents indicated

that actual losses were less than expectations and 37.5% of TMT members shared the same position. Finally, 41.2% of CSO respondents indicated that the estimated loss through theft and recovery costs from security breaches was better than expectations while only 25.0 % of the TMT members shared this position.

5.13 Respondent Descriptive Statistics

The descriptive statistics for the respondents have been summarized in this section of the dissertation. The statistics are reported in the following tables: All respondents (see table 22), TMT members (see table 23), CSOs (see table 24), CIOs (see table 25), and functional managers (see table 26). As shown, only 94% would report their gender. Of the total respondents, at least 80.6% were male. Interestingly, 14.9% of the respondents would not report their age and 70% of these were CSOs and 20% were CIOs. Of those that did report their age, 3.5% were 30 years or less and 45.6% were more than 50 years old. The reported education levels shows that 42.5% of the respondents who answered the question had at least an undergraduate degree. Additionally, 75% of the college graduates had obtained a graduate degree. The group of respondents that had the highest percentage of graduate degrees was the TMT respondents who responded that 43.8% held a graduate degree. The lowest group holding graduate degrees was the CSOs who reported that 11.8% had graduate degrees.

The primary functional responsibility areas for the respondents included a heavy information systems slant. Of the total respondents, 51.5% listed information systems as their primary functional area with finance being represented by 18.2% of the respondents. The inclusion of the CIO and CSO in these figures does distort the overall statistics to a degree. Of the TMT respondents 25.0% indicated that information systems was their primary functional area, and at the functional manager level 26.7% reported that information systems was their primary functional area of responsibility. At these same levels of

management finance as a primary functional responsibility level by 18.8% for TMT respondents and 20.0% at the functional manager level.

5.14 Respondent Work History Statistics

The descriptive statistics for the 67 respondents are summarized in table 27. The table includes the statistics for all respondents, TMT members, CIOs, CSOs, and functional managers. As shown, there is a wide range reported for years employed at the present firm (0.3 to 40 years), present industry (1.0 to 41.0) and present position (0.3 to 25.0). Interestingly, the CSO and CIO respondents reported the highest minimum number of years employed in their industry (3.0), and the CIO respondents reported the lowest minimum time (0.3) in their present position.

On average, the respondents are long time employees of their firms (14.5 years), they have probably come to their present firm from the same industry (20.7 years), and they have held their current position for a considerable amount of time (6.7 years).

5.15 CSO Supplemental Statistics

The 14 CSO respondents who completed this section of the survey have held executive or management positions in general management positions (35.8%) and closely followed by information systems (21.4%). Of the remainder; two held prior managerial positions in accounting; one held a managerial position in marketing; one held a managerial position in sales, one reported a prior executive or managerial position in Risk Management and one reported they held a prior managerial position in general administration.

The 12 CSO respondents, who hold college degrees, graduated with nine bachelor degrees in business, one in engineering, and three in liberal arts. Two hold master's level degrees in business.

5.16 Firm Level Response Rate Interpretation

The population of firms that responded to the survey supplied an interesting mix of data and information that can be interpreted from various perspectives (see table 6). First, the highest percentage response rate recorded (1.8%) was from firms that have employment levels between 500–999. The lowest percentage response rate (1.1%) was from firms with an employment level between 5,000–9,999. This result partially reinforces the decision to focus on firms that had >500 employees and at the same time suggests that large firms with employment >5,000 are not receptive to this type of research study. The discussions that took place during the pilot test phase of the study led to a decision to focus on larger organizations that could afford the costs associated with formal information security programs and that also would be the most likely to have assigned security and risk management personnel. Reviewing the distribution of firm responses rates from the follow-up mailing that solicited reasons for not taking part in the research study reveals that of the 39 firms that identified themselves, 46.2% of the actual responses came from firms that also had the highest percentage (6.1%) response rate based on employment level. The firms with an employment level of 10,000+ were the most willing to identify themselves when they responded as to why they would not take part in the research study.

Reviewing the response rates based on SIC show that the wholesale trade division had the highest response rate (3.3%), followed by the transportation division (2.8%), the construction division (2.4%), the finance and insurance division (2.3%), the manufacturing division (1.2%), the miscellaneous division (0.58%), and the mining division (0.0%). About the only thing that might be extracted from this limited sample is that manufacturing companies have reached a point where they do not want to participate in any additional mail surveys and that the mining industry has no interest in responding to mail surveys.

Additionally, reviewing the results of a recent information security survey conducted by Information Security, The 2000 Information Security Industry Survey, sponsored by ICSA.net and Global Integrity may reinforce the position that firms are becoming extremely reluctant to take part in any mail survey information security research regardless of industry. The ICSA.net/Global Integrity sponsored research used an online survey structure. There were e-mail requests sent to approximately 30,000 Information Security qualified subscribers. The reported results included a comment that 1,897 respondents (6.3%) completed some sections of the survey.

5.17 Firm Level Business Risk Profile

Reviewing the responses from the 16 firms that classified themselves as prospectors, analyzers or defenders combined with what these firms reported about their business risk propensity, reveals that there are differences between how a firm that may be considered a high strategic risk and how they approach the major resource allocation decisions to support their current business strategy. Starting with the three prospectors at the high end of the strategic risk taking continuum indicates that two (67.7%) identified themselves as fairly aggressive in making internal resource associated decisions to support their aggressive external business strategies. Both firms reported aggregated mean scores less than the overall firm level aggregated mean score on this dimension. The two firms aggregated reported mean scores were 22.000 and 19.333 versus the overall reported mean score=23.725. The third firm reported a relatively more conservative style on this dimension mean=27.333. The eight firms that identified themselves as analyzers, who are considered lower level strategic risk takers than prospectors, reported three (37.5%), were fairly aggressive in making internal resource associated decisions to support their less aggressive external business strategies and five (62.5%) were less aggressive. The range recorded by these firms did not exceed the lowest aggregated mean for the prospectors. The most aggressive analyzer aggregated mean score was

21.667. The most conservative analyzer aggregated mean score was 32.000. This was relatively more conservative than the most conservative prospector. Three (60.0%) of the five defender firms reported aggregated mean scores that placed them in a more aggressive position than the total firm mean on this dimension. However, the most aggressive defender aggregated mean score was only slightly more aggressive than the most aggressive analyzer mean=21.333. The most conservative defender aggregated mean score was considerably less conservative than the most conservative analyzer mean=25.500. These data seem to support the positioning of firms along a risk continuum from high/aggressive business risk taking firms to low/conservative business risk taking firms using these two measures of business risk taking.

Coupling the firm IT resource posture data with the firm level business risk profiles by strategic risk category reveals that the use of the IT Resource varies widely amongst the three categories. Only two prospector firms reported on the strategic integration and electronic integration section of the questionnaire. The two firms were dramatically different in their use of the IT resource to support their business strategy. The prospector firm that reported the more aggressive internal resource allocation decision process reported lower levels of strategic integration and electronic integration (SI mean=5.333, EI mean=5.833). Both are considerably higher than the reported aggregated overall firm means for SI and EI. The second prospector firm with the more conservative internal resource allocation decision process reported a much higher level of strategic integration and electronic integration (SI mean=3.111, EI mean=3.333). The patterns that were present in the six analyzer firms and five defender firms that reported on the strategic integration and electronic integration section of the questionnaire show mixed SI and EI usage levels similar to the prospector firms. These results tend to support the position that firms will use their IT Resources in significantly different ways in support of their external business strategy. Furthermore, that firms that may be aggressive strategic risk takers may have managers that practice

conservative internal resource decision making which would be a characteristic of a risk avoidance management style.

CHAPTER VI

CONTRIBUTIONS AND RECOMMENDATIONS

6.0 Introduction

Chapter 6 is divided into major sections that include the contributions of the study, the limitations of the research study, the lessons learned and recommendations to guide future research in this area.

6.1 Contributions of the Study

The results of this study have implications for academia, managers and security practitioners in an area that has not been adequately investigated by IS researchers. The research provides a starting point for the development of theory-based guidelines to manage the SRM program process. This contribution is especially relevant in the IS/IT area since the model may be applicable across a wide area of IS/IT application areas (e.g., EUC, SIS, intranets, extranets). The IS field requires effective ways to monitor program performance in order to develop programs to deal with the potential dissatisfaction levels that firm management and end-users may perceive with IT programs. Overall, understanding how the organizational context, the deployed IT resource and the level of risk propensity firm management will accept should aid IS functions in developing and maintaining strategies to improve the IT planning process.

The researcher has provided a theoretical model that can be further developed and validated to study the process that leads to effective SRM programs. The model incorporates desired expectations in an IS area outside of the EUC domain and incorporated the role of executive management support in a direct relationship in the model (Suh et al., 1994). The framework should provide the academic community additional insights to aid research in other

aspects of IS/IT that require performance metrics when viewed within the context of the sociotechnical perspective (e.g., Liker, Roitman & Roskies, 1987).

The exploratory research study was conducted to develop a theoretically based research model that would be suitable to conduct future research studies that would contribute to the body of knowledge about firm level SRM policy formulation content and process issues. The study was the first known attempt to use procedures that are required to develop valid, reliable research instruments to empirically measure an adequately developed SRM Program construct. The exploratory nature of the research study itself contributed by investigating the SRM program process at the firm level. Several research studies have investigated aspects of the SRM program process using the individual as the unit of analysis and at a functional level unit of analysis. Yet there is very little known about what factors are considered important when organizations implement their SRM programs and how they monitor and evaluate the performance of the program. Additionally, in contrast to most IS consumer satisfaction research this research study investigated consumer satisfaction/success in terms of effectiveness using perceived usefulness and perceived employee involvement as separate surrogate measures. Similarly, very little is known about the influence of organizational fit on the effectiveness of SRM programs. Therefore, the results of the research study contribute to the body of knowledge in this area.

The inclusion of separate functional manager perceptions and CSO perceptions in measuring the effectiveness of the SRM program introduced an indirect way to gauge how successful the security function has been in educating the firm level management about the SR levels the current SRM program had to generate countermeasures to deal with. Using both perceptions, to measure effectiveness, avoids a potential incomplete, biased and misleading indicator at the firm level unit of analysis. The integration of both perspectives provided a much clearer indicator of the SRM program process as an organizational process

that requires total stakeholder involvement. Additionally, the results obtained using multi-respondents (TMT and CSO) to measure the confirmation/disconfirmation construct at each firm clearly shows that at the firm level there can be major differences between how the gap between desired performance and actual performance is perceived. This gap can have a major influence on the future support levels management will provide the information security function. Using both perceptions allows a much clearer view, which contributes to a potentially less biased understanding of the SRM program process. This is an area the security community should investigate and see how they can narrow the gap by taking steps to influence the expectation levels held by firm management relative to the actual performance levels the SRM program can perform at.

An additional contribution of the dissertation is that it establishes a point of reference to develop theory-based principals that security practitioners can use to implement and monitor SRM programs in different organizational contexts. Based on the growing number of reported security breaches it is apparent that using rigid guidelines regardless of the organizational context is not proving successful.

An indirect contribution of the research study is the information that can be extracted from the data collected from the firms that provided reasons for their organizations not taking part in the pilot test phase and the data collection phase of the research study. This type of feedback should prove beneficial for anyone planning to research organizational information security issues.

6.2 Limitations

Due to the earlier reported setbacks experienced during the pilot test stage of the study the original purpose of the research study was not fully accomplished. The research model had several original constructs whose measures had not been validated in previous empirical studies. One of the major goals of the research study was to gain an understanding of the nature of the

constructs and their relationships in the conceptual research model (Sethi & King, 1991). Therefore, the construct validity of the original instruments was an important issue for the study (Subramanian & Nilakanta, 1994).

The research study continued with the anticipation that sufficient data would be collected to empirically test the relationship and relative importance that executive management support, the actual performance of the SRM program and the difference between the expected performance and actual performance have on SRM Program success. The limited response rate reduced the potential benefits associated with the application of descriptive statistical methods to organize and summarize the data and eliminated the use of inferential statistics to estimate population parameters and to test hypotheses.

6.3 Lessons Learned

The response rate experienced with the research study was probably further limited by the recent series of distributed denial of service (DDOS) attacks against highly visible web sites during the past twelve months, the increased levels of reported hacks by crackers on organizational information resources via the internet, and the increased reported numbers of major malicious code attacks on organizational information resources. Taken together, this publicity probably worked against any outside individual attempting to gain information about an organization's security culture.

Additionally, the response rate is probably what can be expected by any researcher submitting information security research questionnaires by mail, to business organizations, without having a major government agency, commercial or professional organization sponsor. The researcher learned that information security research is probably one of the most intrusive types of organization research and that there is probably a general mistrust of any academic "outsider" attempting to gain entry in order to gather data about the actions of the security practitioner community. There were several instances during the data collection

phase of the research study when the researcher was questioned via telephone about why the researcher had an interest in collecting the data and was this only a “passing interest.” The researcher always informed the individuals that the study was part of a research program that had relevance for the security community and in fact, one presentation had been made at a security symposium relative to the research goals. This mode of response was responsibility for at least two firms completing the questionnaires and sending them in. There was one instance when the researcher was told that his credentials had been reviewed with a third party due to concerns the firm had that the researcher may be practicing “social engineering” techniques to gain information about the firm’s SRM program technology countermeasures. These types of encounters reinforce the importance of gaining sponsorship from an organization entity that has credibility with the firms in the industry that the information security research will be conducted. Additionally, that researchers who plan to pursue research in this area must become visible and active in the practitioner community

The researcher learned, the hard way, that in order to develop a research stream in an emerging area requires major personnel, financial and professional commitments far beyond what an individual researcher can afford to expend. The total cost of the research project has exceeded \$10,000 and has required additional personnel and professional tradeoffs that have far exceeded what was originally estimated.

6.4 Future Directions

The process to develop and implement an SRM program is time sensitive. In order to fully explore the process a form of longitudinal research is an appropriate approach to fully capture the process dynamics. The use of case study research would be an appropriate methodology for this firm level process (Yin, 1989). Additionally, the area is new and it is under researched. It may contain several novel, testable, and empirically valid theories (Eisenhardt, 1989). Using the guidelines proposed by Eisenhardt and the additional guidance

provided by Eisenhardt (1991) a multiple case study research strategy should be pursued. The research should use a combination of interviews and questionnaires since multiple individuals are involved in the SRM program process.

The original model constructs should be evaluated in order to ascertain their precision and measurability, which is required for building powerful theory (Eisenhardt, 1991). The research should proceed without any a priori hypotheses in order to be able to capture a full understanding of the how and why realities of the process that leads to the effectiveness outcomes (Yin, 1993). The study should proceed with four to ten cases being included so that theory can be fully developed and yet not be overwhelmed by the massive amounts of data that would be generated from more than ten cases (Eisenhardt, 1989). As the case studies progress the data collected should be analyzed for patterns that might lead to the need for additional types of data to be collected (Cavaye, 1996). Potentially, this iterative methodology might lead to additional or modified research questions (Eisenhardt, 1989). This approach of collecting a variety of in-depth data over the process cycle would do much to enhance the future possibility of establishing causal relationships that would be incorporated in the resulting validated theoretical model. Additionally, using a multi-case strategy will allow a compare and contrast capability in order to deal with possible multi-location firms (Miles & Huberman, 1984). The validated theoretical model should then be suitably operationalized and tested in different organizational contexts in different industries. This would allow the cumulative research results to be evaluated in order to determine if the research results extracted from the model could be generalized and incorporated in the existing IS/IT performance research knowledge base.

TABLES

Table 1. List of Accidental and Intentional Threats to Information

Major Threat Category	Specific Threat Category
Availability and Usefulness	Destroy, damage, or contaminate data Deny, prolong, or delay is of or access to data Move or misplace data Convert data
Confidentiality and Possession	Access data Disclose data Observe data or monitor data and acquire knowledge Copy data Take away or control data Declare ownership or custodianship of data
Integrity and Authenticity	Enter, use, or produce false or harmful data Modify, replace, remove, append, or reorder data Misrepresent data Repudiate (reject as untrue) data Misuse data or fail to use data as required
Exposure to threats	Endanger data by exposure to any of the preceding threats Fail to engage in or allow the preceding threats to occur when desired by the owner of the information

Source: Parker (1995, 1995c)

Table 2. Components of a Security Risk Management Program

Major Category	Dimension and definition
Written Corporate policy [A] [B]	Business objectives and goals include compliance with a board-level security policy,
Systems security policy	This policy lays down basic security requirements of the proposed system that is more or less independent of the final solutions that are developed. It should be major input to systems designers and builders.
Product security policy.	The purchased IT products should come with security Policies similar in content and functionality to a system security policy.
Community security policy.	This policy specifies the security and control requirements for a network or community consisting of two or more computers.
Information security policies :[D]	The policies should include general statements of goals, objectives, beliefs, ethics, and responsibilities, which should be accompanied by the general means for obtaining these things. The policies must establish baseline minimum security/protection level so that all individuals subscribe to some minimal level of protection. Clarification of freedom of information policies and right to privacy must be clarified
Risk analysis/assessment :[B] :[C]	This should be performed prior to establishing the proper controls-mix for an organization and before writing an information security policy for the specific unique organization; formal risk assessment packages to match environment (culture) of organization; specific principals match organization security policy.
Formal periodic reinforcement of the policy principles :[B]	
Proactive security practices :[B]	Penetration testing techniques possibly using social engineering
Risk communications	Security risk information bulletins
Quick reaction teams (QRT)	

Table 2—Continued.

Policy distribution checks :[B]	A formal reappraising of current distribution lists updating what and to whom distribution should be made to.
Management meetings :[B].	The group responsible for publishing security policy should Attend meetings held in key business areas of the organization to discuss the policy
formal published policy :[B] :[D]	Plain English version all employees , various versions for different types of audience levels; end users, managers, Customers, Business Partners, IS department
Data ownership: :[B]	Differentiate between the role of the data owner and the role of the custodian
Specific responsibility assignments :[C]	Who has direct responsibility for issuing and enforcing specific policy.
Security training and awareness efforts :[C].	Policy should clearly identify and define appropriate behavior, demonstrate it's concern, and specify which behaviors are acceptable/unacceptable for future criminal prosecution
Centralized security function mandatory :[C]	
Security Risk Education :[B] :[C]	Commitment of executives, operational managers, manager's subordinates through Education
Status and report level of security function [B]	Organization level will determine influence
Separation of duties :[B]	IT security policymaking and support activities separate from security administration responsibilities; system development process separate from IT security.

Sources:[A] Lindup, 1995; [B] Plant, 1993; [C] Wood, 1995; [D] Wood, 1995b.

Table 3. Definitions of Constructs and Dimensions

Construct: SRM Program: The countermeasures and process available to deal with threats to and vulnerabilities of the IT resource

Dimension: Posture: The content and process responsible for the current countermeasures that provided protection against potential security breaches and the mechanisms required to adjust the current level of security risk management

Source: The major input for the questions are derived from Herold, R. (1994). Case study: An information security program. *Computer Security Journal*, 10(02): 17-26. The article describes content and process issues associated with what dimensions are considered important for information security programs.

Construct: IT Resource: The total hardware, software, networks, and telecommunications capabilities of the firm.

Dimension: Posture: The current internal and external deployment, business utilization and organization of the IT resource by the firm in order to affect organizational effectiveness, shape organizational business and IT governance, and provide connectivity and seamless automatic service sharing.

Source: Adapted from Chan, Y. E. (1992). Business strategy, Information systems strategy, and strategic fit: Measurement and performance impacts. Questionnaire from Ph.D. dissertation section D (Information systems strategy). The section contains a total of 62 questions divided into 4 sections (Dimensions). I have attempted to only select and modify questions I determined would be relevant. Furthermore, I have replaced some of the questions with questions that are more representative of the basic dimensions of level of EI (Venkatraman, 1994) and Reach and Range (Keen, 1991).

Construct: Firm Management Characteristics: The level of concern held by firm management in viewing potential security risks and their consequences based on their knowledge of the countermeasures available from the current SRM program and their risk propensity.

Dimension: Risk Propensity: The firm management position relative to risk as reflected in business resource allocation decisions and in market and product decisions.

Concept: From Venkatraman (1989). Strategic Orientation of Business Enterprises: The Construct, Dimensionality, and Measurement. *Management Science* 15(8): 942-961. The five questions are the same ones used in the article.

Table 3—*Continued.*

Construct: Executive Management Support: The level of executive support as demonstrated by their involvement and participation in the SRM program and their risk propensity.

Concept: from Jarvenpaa & Ives (1991) Executive involvement and participation in the management of information technology. *MIS Quarterly* 15(2): 205-227. The questions were suggested from the awareness and Involvement organizational Assessment checklist from Fisher, 1984 Self -Assessment Checklist

Dimension: Involvement: The degree of importance placed on the security risk management program by the top management of the organization.

Dimension: Participation. Executive activities or substantive personal interventions in the management of the security risk management program.

Construct: Actual Performance of SRM Program: The residual net negative business consequences of the total number of security breaches experienced by the organization, in the past 12 months.

Concept: From Straub, Jr. (1990). *Effective IS Security: An Empirical Study*. *Information Systems Research*. 1(03). Modified from Straub instrument for period of performance and in requesting data in total rather than for every individual security breach. Additionally, relative perceptual measures are substituted for the objective structure developed by Straub.

Dimension: Security Breach Severity: The actual number and impact level of security breaches experienced in the past twelve months relative to other firms in the same industry.

Dimension: Magnitude of Security Breach Costs: The qualitative evaluation of the business impact of security breaches experienced in the past twelve months

Construct: Effectiveness of SRM Program: The extent to which the SRM program actually contributes to achieving organizational goals.

Dimension: Perceived Usefulness: The perceived net benefits from the SRM program toward satisfying tradeoffs of cost, flexibility and ease-of-use goals versus SRM goals.

Table 3—*Continued.*

Dimension: Perceived Employee Involvement: The level of employee cooperation in monitoring and reporting security breaches and in overall compliance with the SRM program

Construct: Confirmation / Disconfirmation: The gap between the desired performance levels and the actual performance levels of the organization security risk management program over the past 12 months. The level of disconfirmation indicates the degree to which perceived actual performance exceeds desired performance

Construct: Desired Performance of SRM Program: The desired residual net negative business consequences of the total number of security breaches expected by the organization during the past 12 months

Dimension: Security Breach Severity: The desired number and impact level of security breaches anticipated over the past twelve months.

Dimension: Magnitude of security Breach Costs: The qualitative estimate of the desired level of the business impact of security breaches expected during the past twelve months

Strategic Archetype: A configuration of contextual, structural and strategic factors that maximizes fit.

Industry: Major business sector the firm competes in.

Structure: The level of flexibility, informality and non-bureaucratic values and principals embedded in the organizational culture.

Source: Covin & Slevan (1988). The influence of organization structure on the utility of an entrepreneurial top management style. *Journal of Management Studies*. 23(3): 217-234.

Size: The number of employees in the organization who are computer users relative to the total number of employees. Additionally, the level of computer resources available for the employees.

Table 4. Research Constructs, Dimensions and Measures
Used in the Data Collection Phase

CONSTRUCT	DIMENSIONS	MEASURES
SRM Program	Posture (Hard ←----→ Soft)	1. Governance [4 questions] 2. Countermeasures [13 questions] 3. Structure [5 questions] 4. Policy and Procedures [19 questions]
IT Resource	Posture (Narrow ←----→ Broad)	1. Strategic Integration [9 questions] 1. EI Level [6 questions] 1. Reach and Range [2 questions]
Firm Management Characteristics	Risk Propensity	1. Business Risk [5 questions]
Executive Management	Involvement	1. 6 questions.
Support	Participation	1. 5 questions.
Actual Performance of SRM Program	Security Breach Severity	1. Number of Security Breaches [1 question] 2. Severity Distribution of Security Breaches [1 question]
Relative to firms in the same industry over the past 12 months	Magnitude of Security Breach Costs.	1. Dollar Cost of Lost Business Opportunity [1 question] 2. Dollar Cost of Theft/Embezzlement [1 question]

Table 4—*Continued.*

Effectiveness of Program	Perceived Usefulness	<ol style="list-style-type: none"> 1. Cost/Security Tradeoff [1 questions] 2. Flexibility/Security Tradeoff [2 questions] 3. Ease-of-Use/Security Tradeoff [2 questions] 4. Relative Usefulness [1 question]
Effectiveness of Program	Perceived Employee Involvement	<ol style="list-style-type: none"> 1. Employee Cooperation [2 questions] 2. Employee Compliance [5 questions]
Confirmation/Disconfirmation	Security Breach Severity	<ol style="list-style-type: none"> 1. Number of Security Breaches [1 question] 2. Severity Distribution of Security Breaches [1 question]
Gap (difference) over the past 12 months	Magnitude of Security Breach Costs	<ol style="list-style-type: none"> 1. Dollar Cost of Lost Business Opportunity [1question] 2. Dollar Cost of Theft/Embezzlement [1 question]
Control Variables	1. Strategic Archetype	1. 1 question
	2. Industry	1. 1 question
	3. Structure	1. 5 questions
	4. Size	<ol style="list-style-type: none"> 1. Number of Employees/Computer Users [3 questions] 2. Computer Resources [1 question]

Table 5. Pilot Test Firm Data

Reason For Refusal	Number	%
Y2K issues require total focus of organization	15	35.7
Job Security Issues	6	14.3
Don't have a formal program	5	11.9
Top management would want explanations	5	11.9
Top management too busy	3	7.0
Recently failed security audit	2	4.8
Don't participate in this type of academic research	2	4.8
No reason given	2	4.8
Information security program details classified sensitive	1	2.4
Lost time cost	1	2.4
TOTAL	42	100.0

Table 6. Response Rates

Firm Response Rate with at Least One Return			
Firms	Total Employees	Responses	%
393	500-999	7	1.8
602	1000-4999	9	1.5
179	5000-9999	2	1.1
300	10000+	5	1.7
1,474		23	1.6
Firm Response Rate with Nonresponse Reasons			
Firms	Total Employees	Responses	%
386	500-999	8	2.1
594	1000-4999	10	1.7
177	5000-9999	3	1.7
295	10000+	18	6.1
NA	NA	35	NA
1,452		74	5.1

Firm Response Rate with at Least One Return

FIRMS	SIC DIVISION	DESCRIPTION	RE-SPONSES	%
44	DIVISION B	MINING	0	0.00
42	DIVISION C	CONSTRUCTION	1	2.40
569	DIVISION D	MANUFACTURING	7	1.20
181	DIVISION E	TRANSPORTATION	5	2.80
91	DIVISION F	WHOLESALE TRADE	3	3.30
203	DIVISION G	RETAIL TRADE	2	0.99
171	DIVISION H	FINANCE, INSURANCE AND OTHER	4	2.30
173	MISC.	NONCLASSIFIED + OTHER	1	0.58
1,474			23	1.60

Table 7. Non Response Feedback from 74 Firms

	Number	%
1. The organization does not accept unsolicited submissions of any ideas or materials	5	6.8
2. The request did not comply with our established policies for survey requests.	0	NA
3. Due to the large volume of survey requests we receive our policy is not to participate in any surveys	19	25.7
4. Due to the large volume of survey requests we receive we cannot participate in every one we receive	22	29.7
5. The corporate headquarters is responsible for such decisions and the survey was forwarded there	4	5.4
6. Temporary issues (company being sold/reorganization is in progress)	6	8.1
8. The university sponsor for the research study cannot provide legal confidentiality protection	1	1.4
9. The use of individual identification numbers on the questionnaires could be used to reveal responses by an individual or by the organization	3	4.1
10. The questionnaires contain some questions that require answers that would reveal proprietary information	7	9.5
11. The questionnaires contain many questions that would require checking company records	3	4.1
12. We do not share any information about our computer security policies with outside entities	17	23.0
13. Our management team is too busy to spend time filling out any survey questionnaires	9	12.2
14. The time of our management team is valuable and we decided that the benefits we would receive for the time expended was not adequate to participate in the research project.	17	23.0
15. Company security policies prevent complete answers to some of the requested information	7	9.5
16. Company policy prevents revealing any demographic information about our management team	4	5.4
17. Company policy prevents revealing any information about our management team business philosophy or internal actions	3	4.1
18. OTHER:	1	1.4
TOTAL	128	

Table 8. IT Resource Posture Strategic Integration

[1] To a Large Extent - [7] Not at All [Descriptive Statistics From 18 Firms]	Mean
1. We offer computer-related products or services to our customers, distributors, or suppliers.	4.778
2. We offer computer-related products or services to our competitors.	6.333
3. We store information in our databases, which is accessed and used by our customers, distributors, or suppliers.	5.333
4. Our computer resources help us build closer ties with other firms.	4.111
5. Information systems technology helps us improve our products and services.	2.278
6. We have computer applications, which support our products.	3.056
7. We have developed computer applications, which are an integral part of our products.	4.056
8. Our computer systems help direct and control production of our product and / or services.	1.944
9. Much of the corporation's competitive position may depend on controlling the information it has.	2.722

Table 9. IT Resource Posture Electronic Integration (EI) Level

[1] To a Large Extent - [7] Not at All [Descriptive Statistics From 18 Firms]	Mean
1. Our computer systems exchange information with our customers/distributors (e.g. electronic payments, order entry, order-tracking).	3.944
2. Our computer systems exchange information with our suppliers (e.g. electronic payments, order entry, order-tracking).	4.889
3. Our computer systems provide inventory status and allow the initiation of an inventory release/build transaction by our customers /distributors.	4.833
4. Our computer systems allow us to check inventory status and allow us to initiate an inventory release/build transaction with our suppliers.	3.889
5. Our computer systems allow us to share business process information with business alliance organizations in order to improve efficiency and effectiveness amongst the group (e.g. design activities with manufacturing processes).	5.333
6. Our computer systems allow us to share knowledge necessary to assess and interpret complex data (e.g. technical, managerial, legal, medical) with specific organizations.	5.222

Table 10. IT Resource Posture Reach

Whom can you easily reach?	Firms	%
Anyone, anywhere	9	50.0
Customers, suppliers with the same IT base as yours	7	38.9
Customers, suppliers regardless of IT base	12	66.7
Across different business units abroad	7	38.9
Across different business units domestically	14	77.8
Across geographically spread single business unit locations	15	83.3
Within a single business unit location	13	72.2

Table 11. IT Resource Posture Range

What services can you share automatically and seamlessly	Firms	%
Perform transactions [complex on multiple applications, i.e., process orders]	13	72.2
Perform transactions [simple, i.e. take orders]	15	83.3
Access to information, i.e. check credit rating	12	66.7
Send messages, i.e. send a memo	18	100.0

Table 12. Business Risk Propensity

[1] Strongly Agree – [7] Strongly Disagree	Descriptive Statistics From 23 Firms	Mean
1.	Our operation can be generally characterized as high risk.	4.355
2.	We seem to adopt a rather conservative view when making major decisions. [reverse scale]	2.993
3.	New projects are approved on a “stage-by-stage” basis rather than with “blanket” approval. [reverse scale]	3.551
4.	We seem to have a tendency to support projects where the expected returns are certain [reverse scale]	3.022
5.	Operations have generally followed the “tried and true” paths [reverse scale]	3.065

Table 13. Organization Structure

Descriptive Statistics from 15 Firms		
	Mean	Semantic differential seven point interval scale
The operating management philosophy of top management of my business unit is		
Tight formal control of most operations by means of sophisticated control and information systems	3.333	Loose, informal control; heavy dependence on informal relations and norm of co-operation for getting work done
Strong emphasis on always getting personnel to follow the formally laid down procedures	2.933	Strong emphasis on getting things done even if this means disregarding formal procedures
A strong emphasis on holding fast to tried and true management principles despite any changes in business conditions	3.733	A strong emphasis on adapting freely to changing circumstances without too much concern for past practice
Strong insistence on a uniform managerial Style throughout the business	4.333	Managers’ operating styles allowed to range freely from the very formal to the very informal
Strong emphasis on getting line and staff personnel to adhere closely to formal job descriptions	3.533	Strong tendency to let the requirements of the situation and the individual’s personality define proper on-job behavior

Table 14. Executive Management Support Involvement

[1] To a large extent – [7] Not at all	Descriptive Statistics From 18 Firms	Mean
1. Senior management has fully supported the establishment of plans, policies, programs, and guidelines for information security.		2.500
2. The information security function is supported with appropriate resources to perform its function in system design, test and evaluation.		3.222
3. Senior management has fully supported the implementation of a comprehensive education and training program in asset protection (data security, information security, contingency planning, and so on.)		3.611
4. Senior management has fully supported the use of risk assessment methods to periodically and objectively demonstrate the degree of security risk.		2.889
5. The firm's business objectives and goals include compliance with a broad-level security policy.		3.176

Table 15. Executive Management Support Participation

[1] To a large extent – [7] not at all	Mean
1. Senior management really understand the terms sensitive data, vital records, security awareness, basic controls, control center, life cycle, EDP audit, disaster / recovery, and adequacy of control as applied to information systems.	2.833
2. Each of the topics in question 1 is addressed by some corporate statement or directive.	3.778
3. Senior management takes an active role in development and implementation of security controls.	4.000
4. Senior management takes an active role in our methodology for identifying exposures, assessing risks, and approving recommended controls for those information systems now used and under current development.	3.889
5. Senior management has been involved in identifying and prioritizing all key systems/applications that are critical to the operation of the business.	3.500

Table 16. Security Policy Development

[1] To a large extent – [7] not at all Descriptive Statistics From 18 Firms	Mean
Our corporate/business level security policy is the result of inputs from many members of our organization, including security officials, line managers, IT resource specialists, and our IT resource user community	3.278
When we formally issued our corporate/business level security policy there was visibility given the event through such devices as management presentations, panel discussions, guest speakers, question/answer forums, a newsletter announcement specifically indicating why the organization was issuing the policy such as the requirements of the Computer Security Act, etc.	4.235
We planned for and budgeted sufficient funds for additional staffing, training, and equipment prior to the formal issuance of the corporate/ business level security policy	4.556

Table 17. Security Policy Process

[1] To a large extent – [7] not at all Descriptive Statistics From 18 Firms	Mean
We utilize risk management techniques (evaluation, analysis, etc.) and audit reviews to periodically assess the degree of risk associated with threats to and vulnerabilities of our information resources	3.111
We use audit reviews to evaluate the levels of risk in order to identify levels that exceed acceptable limits established by management	3.222
System development uses a formal management system to build the organization's information systems	3.667
An external group (function) outside of the IS organization evaluated the basic controls used by the IS organization	3.667
An external group (function) outside of the IS organization periodically evaluates the basic controls used by the IS organization.	3.278
Auditors and security personnel are involved in design changes in information systems	4.000
We utilize penetration testing techniques in order to periodically assess the vulnerability of our information resources	3.889
We have utilized penetration teams using social engineering to periodically assess our security risk management program	4.889
The activities of security administrators are well known to users at this location	3.833
Our security policy is up to date and has been updated to deal with our current security risks	3.611

Table 18. Security Protection Plan

Descriptive Statistics From 18 Firms		
Section Covered	Number of Firms	% of Firms
Systems descriptions	9	50.0
Information security	13	72.2
MIS security	15	83.3
Personnel Security	9	50.0
Communications Security	7	38.8
Physical Security	13	72.2
Contingency plans	9	50.0

Table 19. Security Awareness Training and Accountability

[1] To a large extent – [7] not at all	Descriptive Statistics From 18 Firms	Mean
Our security awareness program employs regular follow-up reminders, e.g., such activities as posters, articles in the company newspaper, issuing follow-up pamphlets, etc.		4.722
Our security awareness program includes soliciting suggestions from our employees on how we can improve the cost/benefit ratio associated with our current security program		5.389
We utilize the security resources available on the Internet to maintain and improve our security awareness and to keep it current. Examples (CERT advisories, Center for Decision Support documentation, etc.).		3.944
Our employee appraisal system includes security policy compliance in performance reviews		5.444
Our functional/departmental managerial appraisal system includes security policy compliance in performance reviews		5.222
We have regular security audits		3.667
We conduct walkarounds to assess employee compliance levels		4.889
We have an established reward for superior security compliance and recommended penalties for security noncompliance		5.833

Table 20. Security Risk Management Program Effectiveness

[1] To a large extent – [7] not at all Descriptive Statistics From 21 Firms	Firm Mean	CSO Mean	FM Mean
We have protective security measures in place that are cost effective and have reduced the level of risk to acceptable levels	2.875	2.778	2.733
The resultant overall security philosophy has been to provide very tight security without hindering productivity	3.125	2.944	3.000
Our firm has the capability to detect attempts to gain unauthorized access to our computer systems	3.227	3.278	3.462
Relative to our type of industry security is very effective at this location	3.000	2.556	3.367
Internal operations that rely on accurate and timely data and information have not been negatively impacted by security measures	3.333	3.444	3.286
Getting information about personal data about employees and clients is time consuming and difficult. [Reverse Scale]	3.458	3.500	3.533
Our security policy requires active enforcement [Reverse Scale]	3.792	3.833	3.533
Our security policy is understood by end users	3.917	4.000	3.933
Our security policy is adhered to by end users	3.458	3.889	3.200
Our security policy is understood by functional management	3.417	3.278	3.600
Our security policy is adhered to by functional management	3.375	3.333	3.400
Data that would be useful to my function is unavailable because we don't have the right authorization			4.800
Getting authorization to access data that would be useful in my function is time consuming and difficult			4.600
We have protective security measures in place that are cost effective and still allow my function to easily do what is required to use the system hardware and software for submitting, accessing, and analyzing data [Reverse Scale]			5.000

Table 21. Confirmation/Disconfirmation

Descriptive Statistics from 20 Firms								
	[-2.0]	[-1.0]	[-0.5]	[0.0]	[+0.5]	[+1.0]	[+1.5]	[+2.0]
[-2] Poorer than desired - [+2] Better than Desired								
The number of security breaches experienced in the last twelve months was								
CSO	0	4		6		2		5
TMT	2	5		4		2		3
FIRM		2	2	4	1	2	1	1
The total estimated value of lost business due to security breaches through lost opportunities was								
CSO	1	1		6		3		6
TMT	0	2		8		4		2
FIRM		1		3	3	5		1
The total estimated loss through theft and/or recovery costs from security breaches was								
CSO	0	4		6		2		5
TMT	0	6		6		2		2
FIRM		1	2	4	3	2		1

Table 22. Demographic Information for All Respondents

Variable	Respondents	%
Gender		
Male	54	85.7
Female	9	14.3
NG	4	NA
Age		
< 30	2	3.5
30 - 40	9	15.8
41 - 50	20	35.1
51 - 60	21	36.8
> 60	5	8.8
NA	10	NA
Education—Highest Educational Level		
Attended High School	0	0.0
High School Graduate	1	1.5
Attended College	13	19.7
College Graduate	28	42.5
Attended Graduate School	3	4.5
Graduate Degree	21	31.8
No Response	1	NA
Primary Functional Responsibility		
Engineering	3	4.5
Finance	12	18.2
Marketing	0	0.0
Manufacturing	1	1.5
Accounting	4	6.1
Sales	0	0.0
Information Systems	34	51.5
President/CEO	3	4.5
General Management	5	7.6
Other	4	6.1
No Response	1	NA

Table 23. Demographic Information for TMT Respondents

Variable	Respondents	%
Gender		
Male	15	100.0
Female	0	0.0
NG	1	NA
Age		
< 30	0	0.0
30 - 40	1	6.7
41 - 50	6	40.0
51 - 60	6	40.0
> 60	2	13.3
NA	1	NA
Education—Highest Educational Level		
Attended High School	0	0.0
High School Graduate	0	0.0
Attended College	1	6.2
College Graduate	7	43.8
Attended Graduate School	1	6.2
Graduate Degree	7	43.8
No Response	NA	NA
Primary Functional Responsibility		
Engineering	0	0.0
Finance	3	18.8
Marketing	0	0.0
Manufacturing	1	6.2
Accounting	1	6.2
Sales	0	0.0
Information Systems	4	25.0
President/CEO	3	18.8
General Management	2	12.5
Other	2	12.5
No Response	NA	NA

Table 24. Demographic Information for CSO Respondents

Variable	Respondents	%
Gender		
Male	12	80.0
Female	3	20.0
NG	3	NA
Age		
< 30	1	9.1
30 - 40	3	27.3
41 - 50	4	36.3
51 - 60	2	18.2
> 60	1	9.1
NA	7	NA
Education—Highest Educational Level		
Attended High School	0	0.0
High School Graduate	0	0.0
Attended College	5	29.4
College Graduate	10	58.8
Attended Graduate School	0	0.0
Graduate Degree	2	11.8
No Response	1	NA
Primary Functional Responsibility		
Engineering	0	0.0
Finance	5	29.4
Marketing	0	0.0
Manufacturing	0	0.0
Accounting	0	0.0
Sales	0	0.0
Information Systems	9	52.9
President/CEO	0	0.0
General Management	1	5.9
Other	2	11.8
No Response	1	NA

Table 25. Demographic Information for CIO Respondents

Variable	Respondents	%
Gender		
Male	14	77.8
Female	4	22.2
NG	0	NA
Age		
30 or <	0	0.0
31 - 40	2	12.5
41 - 50	4	25.0
51 - 60	9	56.2
> 60	1	6.3
NA	2	NA
Education—Highest Educational Level		
Attended High School	0	0.0
High School Graduate	1	5.6
Attended College	4	22.2
College Graduate	5	27.8
Attended Graduate School	1	5.6
Graduate Degree	7	38.8
No Response	0	NA
Primary Functional Responsibility		
Engineering	0	0.0
Finance	1	5.6
Marketing	0	0.0
Manufacturing	0	0.0
Accounting	0	0.0
Sales	0	0.0
Information Systems	17	94.4
President/CEO	0	0.0
General Management	0	0.0
Other	0	0.0
No Response	NA	NA

Table 26. Demographic Information for Function Manager Respondents

Variable	Respondents	%
Gender		
Male	13	86.7
Female	2	13.3
NG	0	NA
Age		
30 or <	1	6.7
31 - 40	3	20.0
41 - 50	6	40.0
51 - 60	4	26.6
> 60	1	6.7
NA	0	NA
Education—Highest Educational Level		
Attended High School	0	0.0
High School Graduate	0	0.0
Attended College	3	20.0
College Graduate	6	40.0
Attended Graduate School	1	6.7
Graduate Degree	5	33.3
No Response	0	NA
Primary Functional Responsibility		
Engineering	3	20.0
Finance	3	20.0
Marketing	0	0.0
Manufacturing	0	0.0
Accounting	3	20.0
Sales	0	0.0
Information Systems	4	26.7
President/CEO	0	4.5
General Management	2	13.3
Other	0	0.0
No Response	NA	NA

Table 27. Employment History for Respondents
Data from 65 Respondents

Years Employed	# Respondents	Average	Minimum	Maximum
All Respondents				
Present Firm	65	14.5	0.3	40.0
Present Industry	65	20.7	1.0	41.0
Present Position	65	6.7	0.3	25.0
NG	2	NA	NA	NA
TMT Respondents				
Present Firm	16	16.6	1.0	37.0
Present Industry	16	21.1	1.0	40.0
Present Position	16	5.7	1.0	24.0
NG	NA	NA	NA	NA
CSO Respondents				
Present Firm	17	16.6	1.0	35.0
Present Industry	17	19.1	3.0	35.0
Present Position	17	7.4	1.0	20.0
NG	1	NA	NA	NA
FM Respondents				
Present Firm	14	11.5	1.0	27.0
Present Industry	14	17.5	1.0	41.0
Present Position	14	6.8	1.0	25.0
NG	1	NA	NA	NA
CIO Respondents				
Present Firm	18	12.9	0.3	40.0
Present Industry	18	24.5	3.0	40.0
Present Position	18	6.8	0.3	23.0
NG	NA	NA	NA	NA

APPENDIX A
RESEARCH SURVEY INSTRUMENTS

CENTER FOR INFORMATION
TECHNOLOGIES MANAGEMENT

THE UNIVERSITY OF TEXAS
AT ARLINGTON



SECURITY RISK MANAGEMENT
RESEARCH PROJECT

CHIEF SECURITY OFFICIAL

THE PURPOSE OF THIS QUESTIONNAIRE IS TO OBTAIN INFORMATION ON COMPANY SECURITY RISK MANAGEMENT PROGRAMS. ALL INFORMATION WILL BE HELD IN STRICT CONFIDENCE, AS HAS ALWAYS BEEN THE POLICY OF THE UNIVERSITY OF TEXAS AT ARLINGTON WITH SPONSORED RESEARCH. WHEN THE RESULTS OF THIS STUDY ARE PUBLISHED, IT WILL BE IMPOSSIBLE TO IDENTIFY SPECIFIC INDIVIDUALS OR FIRMS.

WHEN YOU HAVE COMPLETED THE QUESTIONNAIRE, PLEASE SEAL IT IN THE ATTACHED ENVELOPE FOR MAILING TO THE LOCATION THAT WILL BE PROCESSING THE DATA.

THANK YOU FOR YOUR HELP.

SECURITY RISK MANAGEMENT PROGRAM

Please answer the following questions about specific aspects of your firm's security risk management program. (CSO)

Please respond by circling the correct digit unless otherwise noted.

Policy and Procedures		
1. We have a corporate/business level published security policy.	<input type="checkbox"/> Yes	<input type="checkbox"/> No
2. We have someone as the designated spokesperson in the event that a public announcement has to be made relating to information security.	<input type="checkbox"/> Yes	<input type="checkbox"/> No
3. We have a liaison arrangement with the following. Please check all that apply.	<input type="checkbox"/> human resources <input type="checkbox"/> facility management functions <input type="checkbox"/> corporate security	<input type="checkbox"/> insurance company <input type="checkbox"/> law enforcement agencies <input type="checkbox"/> other _____
4. We have a security protection plan for the organization, which includes the following sections: Please check off all that apply.	<input type="checkbox"/> systems descriptions <input type="checkbox"/> information security <input type="checkbox"/> MIS security <input type="checkbox"/> personnel security	<input type="checkbox"/> communications security <input type="checkbox"/> physical security <input type="checkbox"/> Contingency Plans
5. We have a designated security quick reaction team and when we have a security crisis they are immediately called into action.	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	To a large extent	Not at all
6. Our corporate/business level security policy is the result of inputs from many members of our organization, including security officials, line managers, IT resource specialists, and our IT resource user community.	1	2 3 4 5 6 7
7. When we formally issued our corporate/business level security policy there was visibility given the event through such devices as management presentations, panel discussions, guest speakers, question/answer forums, a newsletter announcement specifically indicating why the organization was issuing the policy such as the requirements of the Computer Security Act, etc.	1	2 3 4 5 6 7
8. We planned for and budgeted sufficient funds for additional staffing, training, and equipment prior to the formal issuance of the corporate/ business level security policy.	1	2 3 4 5 6 7
Policies and Procedures	Too a large extent	Not at all
9. We utilize risk management techniques (evaluation, analysis, etc.) and audit reviews to periodically assess the degree of risk associated with threats to and vulnerabilities of our information resources.	1	2 3 4 5 6 7
10. We use audit reviews to evaluate the levels of risk in order to identify levels that exceed acceptable limits established by management.	1	2 3 4 5 6 7

11. System development uses a formal management system to build the organization's information systems.	1	2	3	4	5	6	7
12. An external group (function) outside of the IS organization evaluated the basic controls used by the IS organization.	1	2	3	4	5	6	7
13. An external group (function) outside of the IS organization periodically evaluates the basic controls used by the IS organization.	1	2	3	4	5	6	7
14. Auditors and security personnel are involved in design changes in information systems.	1	2	3	4	5	6	7
15. We utilize penetration testing techniques in order to periodically access the vulnerability of our information resources.	1	2	3	4	5	6	7
16. We have utilized penetration teams using social engineering to periodically access our security risk management program.	1	2	3	4	5	6	7
17. The activities of security administrators are well known to users at this location.	1	2	3	4	5	6	7
18. Our security policy is up to date and has been updated to deal with our current security risks.	1	2	3	4	5	6	7
19. The last time the security policy was updated was	<input type="checkbox"/> within the last 3 months <input type="checkbox"/> within the last 6 months <input type="checkbox"/> within the last 12 months <input type="checkbox"/> 1 to 2 years			<input type="checkbox"/> more than 2 years <input type="checkbox"/> never <input type="checkbox"/> don't know			
Accountability	To a large extent			Not at all			
1. Our employee appraisal system includes security policy compliance in performance reviews.	1	2	3	4	5	6	7
2. Our functional/departmental managerial appraisal system includes security policy compliance in performance reviews.	1	2	3	4	5	6	7
3. We have regular security audits.	1	2	3	4	5	6	7
4. We conduct walkarounds to assess employee compliance levels.	1	2	3	4	5	6	7
5. We have an established reward for superior security compliance and recommended penalties for security noncompliance.	1	2	3	4	5	6	7
Security Awareness							
1 We have a corporate/business level security awareness program.	<input type="checkbox"/> Yes			<input type="checkbox"/> No			
2 Our security awareness program has established goals by which we can determine effectiveness.	<input type="checkbox"/> Yes			<input type="checkbox"/> No			

<p>3. Please identify the current security awareness program goals, select all which may be included :</p>	<input type="checkbox"/> having passwords changed more frequently <input type="checkbox"/> having security features designed into systems and procedures <input type="checkbox"/> reducing the number of errors <input type="checkbox"/> maintaining better password control <input type="checkbox"/> getting employees to understand and appreciate the value and the sensitivity of the information they handle	<input type="checkbox"/> achieving better audits <input type="checkbox"/> observing better attitudes toward security <input type="checkbox"/> observing better acceptance of the security measures <input type="checkbox"/> other (please specify) <hr/> <hr/>
<p>3. We have a security hotline where employees can report suspected security breaches and be insured that their identity is not revealed?</p>		<input type="checkbox"/> Yes <input type="checkbox"/> No
<p>Training</p>		<p>To a large extent Not at all</p>
<p>4. Our security awareness program employs regular follow-up reminders, e.g., such activities as posters, articles in the company newspaper, issuing follow-up pamphlets, etc.</p>		<p>1 2 3 4 5 6 7</p>
<p>5. Our security awareness program includes soliciting suggestions from our employees on how we can improve the cost/benefit ratio associated with our current security program.</p>		<p>1 2 3 4 5 6 7</p>
<p>6. We utilize the security resources available on the Internet to maintain and improve our security awareness and to keep it current. examples (CERT advisories, Center for Decision Support documentation, etc.).</p>		<p>1 2 3 4 5 6 7</p>
<p>7. The current security awareness program effort was in reaction in large part to actual or suspected past instances of security breaches at this location.</p>		<p>1 2 3 4 5 6 7</p>
<p>Technology (cso)</p>		<p>To a large extent Not at all</p>
<p>1. We have protective measures in place that are cost-effective and have reduced the level of risk to acceptable levels.</p>		<p>1 2 3 4 5 6 7</p>
<p>2. We have technology [software/hardware] in place for the following (check off all that apply)</p>	<input type="checkbox"/> virus protection <input type="checkbox"/> data encryption <input type="checkbox"/> computer access control <input type="checkbox"/> e-mail security <input type="checkbox"/> network security <input type="checkbox"/> single sign-on <input type="checkbox"/> physical security <input type="checkbox"/> biometrics <input type="checkbox"/> back-up storage	<input type="checkbox"/> fax encryption <input type="checkbox"/> database-file security <input type="checkbox"/> authentication tokens <input type="checkbox"/> Internet firewall <input type="checkbox"/> secure modems <input type="checkbox"/> Intranet firewall <input type="checkbox"/> Activity logs <input type="checkbox"/> Other (please list) <hr/>

Security Organization		Very centralized						Very decentralized
1. Organization of the unit's Information Security Services with respect to <i>personnel who carry out security policy related work.</i>		1	2	3	4	5	6	7
2. Organization of the unit's Information Security Services with respect to <i>other personnel, e. g., those administering training, security awareness program, security audits, etc.</i>		1	2	3	4	5	6	7
3. Organization of the unit's Information Security Services with respect to <i>security hardware and software.</i>		1	2	3	4	5	6	7
4. Who is the person with the primary responsibility for information security in the organization?	<input type="checkbox"/> CEO/President							<input type="checkbox"/> Internal Audit director
	<input type="checkbox"/> Staff level							<input type="checkbox"/> MIS Director
	<input type="checkbox"/> Corporate Security Director	<input type="checkbox"/> Nobody						
	<input type="checkbox"/> Business unit manager	<input type="checkbox"/> Information Security officer						
	<input type="checkbox"/> CIO	<input type="checkbox"/> VP level						
	<input type="checkbox"/> IS Audit director	<input type="checkbox"/> Other (Please) list title						
	<input type="checkbox"/> CFO/Controller	_____						

EXECUTIVE MANAGEMENT SUPPORT

Please answer the following questions about your firm's executive management support for the SRM program. Always answer the question using a 1 to 7 scale by circling the correct digit unless otherwise noted. (cso)

Involvement	To a large extent						Not at all	
1. Senior management has fully supported the establishment of plans, policies, programs, and guidelines for information security.	1	2	3	4	5	6	7	
2. The information security function is supported with appropriate resources to perform its function in system design, test and evaluation.	1	2	3	4	5	6	7	
3. Senior management has fully supported the implementation of a comprehensive education and training program in asset protection (data security, information security, contingency planning, and so on.)	1	2	3	4	5	6	7	
4. Senior management has fully supported the use of risk assessment methods to periodically and objectively demonstrate the degree of security risk.	1	2	3	4	5	6	7	
5. The firm's business objectives and goals include compliance with a broad-level security policy.	1	2	3	4	5	6	7	
6. Who is the person (sponsor) who has actively supported information security interests within the organization?	<input type="checkbox"/> CEO/President							<input type="checkbox"/> MIS Director
	<input type="checkbox"/> Business unit manager							<input type="checkbox"/> Staff level
	<input type="checkbox"/> Corporate Security Director	<input type="checkbox"/> Information Security officer						
	<input type="checkbox"/> IS Audit director	<input type="checkbox"/> VP level						
	<input type="checkbox"/> CIO	<input type="checkbox"/> Nobody						
	<input type="checkbox"/> Internal Audit director	<input type="checkbox"/> Other (Please) list title						
	<input type="checkbox"/> CFO/Controller	_____						

Participation	To a large extent						Not at all
1. Senior management really understand the terms sensitive data, vital records, security awareness, basic controls, control center, life cycle, EDP audit, disaster / recovery, and adequacy of control as applied to information systems.	1	2	3	4	5	6	7
2. Each of the topics in question 1 is addressed by some corporate statement or directive.	1	2	3	4	5	6	7
3. Senior management takes an active role in development and implementation of security controls.	1	2	3	4	5	6	7
4. Senior management takes an active role in our methodology for identifying exposures, assessing risks, and approving recommended controls for those information systems now used and under current development.	1	2	3	4	5	6	7
5. Senior management has been involved in identifying and prioritizing all key systems/applications that are critical to the operation of the business.	1	2	3	4	5	6	7

SECURITY RISK MANAGEMENT PROGRAM (SRM) PERFORMANCE

Please answer the following questions about the performance of your firm's SRM program. (cso)

Always answer the question using a 1 to 5 scale by circling the correct digit unless otherwise noted.

Security Breach Severity [Last twelve months]	Extremely low				Extremely high
1. Relative to our type of industry the number of security breaches at this location experienced in the last twelve months would be considered	1	2	3	4	5
2. Relative to your industry can you estimate how your firm compared by severity level of security breaches experienced in the last twelve months					
Extremely serious	1	2	3	4	5
Serious	1	2	3	4	5
of minimal importance	1	2	3	4	5
of negligible importance	1	2	3	4	5
nuisance type	1	2	3	4	5

Magnitude of Security Breach Costs [Last twelve months]	Extremely low					Extremely high				
1. Relative to your industry can you estimate how your firm compared to similar firms in your industry in terms of the total estimated value of lost business due to these security breaches through lost opportunities.	1	2	3	4	5					
2. Relative to your industry can you estimate how your firm compared to similar firms in your industry in terms of the total estimated loss through theft and/or recovery costs from these security breaches.	1	2	3	4	5					

SECURITY RISK MANAGEMENT PROGRAM EFFECTIVENESS

The following items solicit your opinions about how effective your firm's security risk management (SRM) program has been over the past twelve months.

Always answer the question using a 1 to 7 scale by circling the correct digit unless otherwise noted.

Perceived Usefulness	To a large extent						Not at all					
1 We have protective security measures in place that are cost effective and have reduced the level of risk to acceptable levels.	1	2	3	4	5	6	7					
2 The resultant overall security philosophy has been to provide very tight security without hindering productivity.	1	2	3	4	5	6	7					
3 Our firm has the capability to detect attempts to gain unauthorized access to our computer systems.	1	2	3	4	5	6	7					
Perceived Usefulness	To a large extent						Not at all					
4 Relative to our type of industry security is very effective at this location.	1	2	3	4	5	6	7					
5 Internal operations that rely on accurate and timely data and information have not been negatively impacted by security measures.	1	2	3	4	5	6	7					
6 Getting information about personal data about employees and clients is time consuming and difficult.	1	2	3	4	5	6	7					
Employee Compliance	To a large extent						Not at all					
1. Our security policy requires active enforcement	1	2	3	4	5	6	7					
2. Our security policy is understood by end users	1	2	3	4	5	6	7					
3. Our security policy is adhered to by end users	1	2	3	4	5	6	7					
4. Our security policy is understood by functional management	1	2	3	4	5	6	7					
5. Our security policy is adhered to by functional management	1	2	3	4	5	6	7					

Employee Cooperation		
1. In the last twelve months known security breaches were discovered (choose as many as applicable and please put in rank order as to number)	___ by an employee who observed or suspected the security breach	___ through a security or internal/EDP audit
	___ by accident by an employee	___ through normal systems controls, software or procedural
	___ by accident by a IS staff member, security administrator or an internal/EDP audit	___ by an external security audit or external auditor
	___ through a security investigation other than an audit	___ not sure
		___ other (please specify)

CONFIRMATION/DISCONFIRMATION

The following questions ask about how your firm's security risk management (SRM) program performance compared against what was desired from it.

Always answer the question using a -2 to +2 scale by circling the correct digit unless otherwise noted. (cso)

Security Breach Severity [Last twelve months]	Poorer than desired	A little poorer than desired	Just as desired	A little better than desired	Better than desired
1 The number of security breaches experienced in the last twelve months was	-2	-1	0	+1	+2
2 The security breaches experienced in the last twelve months by severity level were					
Extremely serious	-2	-1	0	+1	+2
Serious	-2	-1	0	+1	+2
of minimal importance	-2	-1	0	+1	+2
of negligible importance	-2	-1	0	+1	+2
Nuisance type	-2	-1	0	+1	+2

Security Breach Cost [Last twelve months]					
1. The total estimated value of lost business due to security breaches through lost opportunities was	-2	-1	0	+1	+2
2. The total estimated loss through theft and/or recovery costs from security breaches was	-2	-1	0	+1	+2

Finally we would like to ask you a few questions about your background. Again, all responses are confidential. (cso)

1	How many years have you been employed by your present firm?	
2	How many years of work experience do you have in your present industry?	
3	How many years have you been in your present position in your company?	
4	What would you consider to be your primary functional responsibility at the present time? (check <u>one</u> only)	<input type="checkbox"/> Engineering <input type="checkbox"/> Finance <input type="checkbox"/> Marketing <input type="checkbox"/> Manufacturing <input type="checkbox"/> Other (please write in) <input type="checkbox"/> Accounting <input type="checkbox"/> Sales <input type="checkbox"/> Information Systems <input type="checkbox"/> President/CEO <input type="checkbox"/> General Management
5	In which of the following areas of functional responsibility have you held an executive or managerial position? (check as many as appropriate)	<input type="checkbox"/> Engineering <input type="checkbox"/> Finance <input type="checkbox"/> Marketing <input type="checkbox"/> Manufacturing <input type="checkbox"/> Other (please write in) <input type="checkbox"/> Accounting <input type="checkbox"/> Sales <input type="checkbox"/> Information Systems <input type="checkbox"/> President/CEO <input type="checkbox"/> General Management
6	Your Age: _____	7. Gender <input type="checkbox"/> Male <input type="checkbox"/> Female
8	What is your highest level of education completed? (check only one)	<input type="checkbox"/> Attended high school <input type="checkbox"/> High school graduate <input type="checkbox"/> Attended college <input type="checkbox"/> College graduate <input type="checkbox"/> Attended graduate school <input type="checkbox"/> Obtained graduate degree
9	Do you have a college degree in (check as many as appropriate)	<input type="checkbox"/> Business <input type="checkbox"/> Bachelor _____ Year <input type="checkbox"/> Master _____ Year <input type="checkbox"/> Liberal Arts <input type="checkbox"/> Bachelor _____ Year <input type="checkbox"/> Master _____ Year <input type="checkbox"/> Engineering <input type="checkbox"/> Bachelor _____ Year <input type="checkbox"/> Master _____ Year <input type="checkbox"/> Other (please write in) _____ Year

THANK YOU FOR YOUR COOPERATION!

Approximately how long did it take you to complete this questionnaire? _____ minutes. (cso)
 _____ This number is for analytical purposes only. Again, all responses will be held in strict confidence.

CENTER FOR INFORMATION
TECHNOLOGIES MANAGEMENT

THE UNIVERSITY OF TEXAS
AT ARLINGTON



SECURITY RISK MANAGEMENT
RESEARCH PROJECT

TOP MANAGEMENT TEAM MEMBER

THE PURPOSE OF THIS QUESTIONNAIRE IS TO OBTAIN INFORMATION ON COMPANY SECURITY RISK MANAGEMENT PROGRAMS. ALL INFORMATION WILL BE HELD IN STRICT CONFIDENCE, AS HAS ALWAYS BEEN THE POLICY OF THE UNIVERSITY OF TEXAS AT ARLINGTON WITH SPONSORED RESEARCH. WHEN THE RESULTS OF THIS STUDY ARE PUBLISHED, IT WILL BE IMPOSSIBLE TO IDENTIFY SPECIFIC INDIVIDUALS OR FIRMS.

WHEN YOU HAVE COMPLETED THE QUESTIONNAIRE, PLEASE SEAL IT IN THE ATTACHED ENVELOPE FOR MAILING TO THE LOCATION THAT WILL BE PROCESSING THE DATA.

THANK YOU FOR YOUR HELP.

RISK PROPENSITY

The following items ask about how your firm conducts business in its primary industry. (tmt)

Always answer the question using a 1 to 7 scale by **circling** the correct digit unless otherwise noted.

Business Risk	Strongly agree				Strongly disagree		
1 Our operation can be generally characterized as high risk.	1	2	3	4	5	6	7
2 We seem to adopt a rather conservative view when making major decisions.	1	2	3	4	5	6	7
3 New projects are approved on a "stage-by-stage" basis rather than with "blanket" approval.	1	2	3	4	5	6	7
4 We seem to have a tendency to support projects where the expected returns are certain.	1	2	3	4	5	6	7
5 Operations have generally followed the "tried and true" paths.	1	2	3	4	5	6	7

Strategic Archetype	Please circle the number of the one statement that best describes the way you compete in your main business.
1	We've attempted to locate and maintain a secure niche in a relatively stable product or service area. We've tried to offer a more limited range of products or services than our competitors, and we've tried to protect our domain by offering higher quality and superior service. We may not be at the forefront of developments in the industry, but we have attempted to concentrate instead on doing the best job possible in our market.
2	We've tried to operate within a broad product-market domain that undergoes periodic redefinition. We've wanted to be 'first in' with new products and market areas even if not all of these efforts have proven to be highly profitable. We've tried to respond rapidly to early signals concerning areas of opportunity, and these responses have often led us to a new round of competitive actions.
3	We've attempted to maintain a stable, limited line of products or services, while at the same time we have tried to move out quickly to follow a carefully selected set of the more promising new developments in the industry. We are seldom 'first in' with new products or services, but by carefully monitoring the actions of major competitors in areas compatible with our stable product-market base we try to be 'second in' with a more cost-efficient product or service.
4	We've not been able to have a consistent product-market orientation. We have not been able to be as aggressive in maintaining established products and markets as have our competitors, and we have not been able to take as many risks as they have. We have been forced to respond to environmental pressures.

Industry		
1 What type of industry category best describes your organization's primary and secondary businesses? (Please write a "P" in the box provided next to your Primary business and an "S" next to your Secondary businesses, if applicable.)	<input type="checkbox"/> Agricultural <input type="checkbox"/> Insurance <input type="checkbox"/> Architectural/Engineering Firm <input type="checkbox"/> News Media <input type="checkbox"/> Communication Service <input type="checkbox"/> Oil, Gas, or Mining Extraction <input type="checkbox"/> Distribution/Warehousing <input type="checkbox"/> Pharmaceutical <input type="checkbox"/> Educational Institution <input type="checkbox"/> Public Relations <input type="checkbox"/> Entertainment or Sports <input type="checkbox"/> Real Estate <input type="checkbox"/> Environmental	
	<input type="checkbox"/> Retail <input type="checkbox"/> Food Service <input type="checkbox"/> Research & Development <input type="checkbox"/> Financial Institution <input type="checkbox"/> Security Consulting Firm <input type="checkbox"/> Health Care <input type="checkbox"/> Security Service, Guards and Alarms <input type="checkbox"/> Hotel/Motel/Resort <input type="checkbox"/> Transportation/Travel <input type="checkbox"/> Industrial/Manufacturing <input type="checkbox"/> Utilities <input type="checkbox"/> Other (Please specify.)	
	1a If you identified a primary industry and one or more secondary industry businesses would you please estimate the percentage of your total firm sales generated in the primary industry.	<input type="text"/> %

CONFIRMATION/DISCONFIRMATION

The following items ask about how your firm's security risk management (SRM) program performance compared against what was desired from it. (tmt)

Always answer the question using a -2 to +2 scale by circling the correct digit unless otherwise noted.

Security Breach Severity [Last twelve months]	Poorer than desired	A little poorer than desired	Just as desired	A little better than desired	Better than desired
1 The number of security breaches experienced in the last twelve months was	-2	-1	0	+1	+2
2 The security breaches experienced in the last twelve months by severity level were					
Extremely serious	-2	-1	0	+1	+2
Serious	-2	-1	0	+1	+2
of minimal importance	-2	-1	0	+1	+2
of negligible importance	-2	-1	0	+1	+2
Nuisance type	-2	-1	0	+1	+2

Security Breach Cost [Last twelve months]						
1	The total estimated value of lost business due to security breaches through lost opportunities was	-2	-1	0	+1	+2
2	The total estimated loss through theft and/or recovery costs from security breaches was	-2	-1	0	+1	+2
Finally we would like to ask you a few questions about your background. Again, all responses are confidential. (tmt)						
1	How many years have you been employed by your present firm?					
2	How many years of work experience do you have in your present industry?					
3	How many years have you been in your present position in your company?					
4	What would you consider to be your primary functional responsibility at the present time? (check <u>one</u> only)	<input type="checkbox"/> Engineering	<input type="checkbox"/> Finance	<input type="checkbox"/> Marketing	<input type="checkbox"/> Manufacturing	<input type="checkbox"/> Other (please write in)
		<input type="checkbox"/> Accounting	<input type="checkbox"/> Sales	<input type="checkbox"/> Information Systems	<input type="checkbox"/> President/CEO	<input type="checkbox"/> General Management
5	In which of the following areas of functional responsibility have you held an executive or managerial position? (check as many as appropriate)	<input type="checkbox"/> Engineering	<input type="checkbox"/> Finance	<input type="checkbox"/> Marketing	<input type="checkbox"/> Manufacturing	<input type="checkbox"/> Other (please write in)
		<input type="checkbox"/> Accounting	<input type="checkbox"/> Sales	<input type="checkbox"/> Information Systems	<input type="checkbox"/> President/CEO	<input type="checkbox"/> General Management
6	Your Age: _____	7. Gender		<input type="checkbox"/> Male	<input type="checkbox"/> Female	
8	What is your highest level of education completed? (check only one)	<input type="checkbox"/> Attended high school	<input type="checkbox"/> High school graduate	<input type="checkbox"/> Attended college	<input type="checkbox"/> College graduate	<input type="checkbox"/> Attended graduate school
					<input type="checkbox"/> Obtained grad degree	
9	Do you have a college degree in (check as many as appropriate)	<input type="checkbox"/> Business	<input type="checkbox"/> Bachelor _____ Year	<input type="checkbox"/> Master _____ Year	<input type="checkbox"/> Liberal Arts	<input type="checkbox"/> Bachelor _____ Year
		<input type="checkbox"/> Engineering	<input type="checkbox"/> Bachelor _____ Year	<input type="checkbox"/> Master _____ Year	<input type="checkbox"/> Master _____ Year	<input type="checkbox"/> Other (please write in)
						_____ Year

THANK YOU FOR YOUR COOPERATION!

Approximately how long did it take you to complete this questionnaire? _____ minutes.

_____ This number is for analytical purposes only. Again, all responses will be held in strict confidence.

CENTER FOR INFORMATION
TECHNOLOGIES MANAGEMENT

THE UNIVERSITY OF TEXAS
AT ARLINGTON



SECURITY RISK MANAGEMENT
RESEARCH PROJECT

FUNCTIONAL MANAGER

THE PURPOSE OF THIS QUESTIONNAIRE IS TO OBTAIN INFORMATION ON COMPANY SECURITY RISK MANAGEMENT PROGRAMS. ALL INFORMATION WILL BE HELD IN STRICT CONFIDENCE, AS HAS ALWAYS BEEN THE POLICY OF THE UNIVERSITY OF TEXAS AT ARLINGTON WITH SPONSORED RESEARCH. WHEN THE RESULTS OF THIS STUDY ARE PUBLISHED, IT WILL BE IMPOSSIBLE TO IDENTIFY SPECIFIC INDIVIDUALS OR FIRMS.

WHEN YOU HAVE COMPLETED THE QUESTIONNAIRE, PLEASE SEAL IT IN THE ATTACHED ENVELOPE FOR MAILING TO THE LOCATION THAT WILL BE PROCESSING THE DATA.

THANK YOU FOR YOUR HELP.

STRUCTURE

The following items solicit your opinions about managerial and organizational characteristics of your firm. (fm)

Always answer the question using a 1 to 7 scale by **circling** the correct digit.

The operating management philosophy of top management of my business unit is		
Tight formal control of most operations by means of sophisticated control and information systems	1 2 3 4 5 6 7	Loose, informal control; heavy dependence on informal relations and norm of co-operation for getting work done
Strong emphasis on always getting personnel to follow the formally laid down procedures	1 2 3 4 5 6 7	Strong emphasis on getting things done even if this means disregarding formal procedures
A strong emphasis on holding fast to tried and true management principles despite any changes in business conditions	1 2 3 4 5 6 7	A strong emphasis on adapting freely to changing circumstances without too much concern for past practice
Strong insistence on a uniform managerial Style throughout the business	1 2 3 4 5 6 7	Managers' operating styles allowed to range freely from the very formal to the very informal
Strong emphasis on getting line and staff personnel to adhere closely to formal job descriptions	1 2 3 4 5 6 7	Strong tendency to let the requirements of the situation and the individual's personality define proper on-job behavior

SECURITY RISK MANAGEMENT PROGRAM EFFECTIVENESS

The following items solicit your opinions about how effective your firm's security risk management (SRM) program has been over the past twelve months. (fm)

Always answer the question using a 1 to 7 scale by **circling** the correct digit unless otherwise noted.

Perceived Usefulness	To a large extent	Not at all
1 We have protective security measures in place that are cost effective and have reduced the level of risk to acceptable levels.	1 2 3 4 5 6 7	
2 The resultant overall security philosophy has been to provide very tight security without hindering productivity.	1 2 3 4 5 6 7	
3 Data that would be useful to my function is unavailable because we don't have the right authorization.	1 2 3 4 5 6 7	
4 Getting authorization to access data that would be useful in my function is time consuming and difficult.	1 2 3 4 5 6 7	

5 We have protective security measures in place that are cost effective and still allow my function to easily do what is required to use the system hardware and software for submitting, accessing, and analyzing data.	1	2	3	4	5	6	7
6 Our firm has the capability to detect attempts to gain unauthorized access to our computer systems.	1	2	3	4	5	6	7
7 Relative to our type of industry, security is very effective at this location.	1	2	3	4	5	6	7
8 Internal operations that rely on accurate and timely data and information have not been negatively impacted by security measures.	1	2	3	4	5	6	7
9 Getting personal data about employees and clients is time consuming and difficult.	1	2	3	4	5	6	7

RISK PROPENSITY

The following items ask about how your firm conducts business in its primary industry. (fm)

Always answer the question using a 1 to 7 scale by circling the correct digit unless otherwise noted.

Business Risk	Strongly agree						Strongly disagree
1 Our operation can be generally characterized as high risk.	1	2	3	4	5	6	7
2 We seem to adopt a rather conservative view when making major decisions.	1	2	3	4	5	6	7
3 New projects are approved on a "stage-by-stage" basis rather than with "blanket" approval.	1	2	3	4	5	6	7
4 We seem to have a tendency to support projects where the expected returns are certain.	1	2	3	4	5	6	7
5 Operations have generally followed the "tried and true" paths.	1	2	3	4	5	6	7
Employee Compliance	To a large extent						
1 Our security policy requires active enforcement	1	2	3	4	5	6	7
2 Our security policy is understood by end users	1	2	3	4	5	6	7
3 Our security policy is adhered to by end users	1	2	3	4	5	6	7
4 Our security policy is understood by functional management	1	2	3	4	5	6	7
5 Our security policy is adhered to by functional management	1	2	3	4	5	6	7

Finally we would like to ask you a few questions about your background. Again, all responses are confidential. (fm)		
1	How many years have you been employed by your present firm?	
2	How many years of work experience do you have in your present industry?	
3	How many years have you been in your present position in your company?	
4	What would you consider to be your primary functional responsibility at the present time? (check <u>one</u> only)	<input type="checkbox"/> Engineering <input type="checkbox"/> Finance <input type="checkbox"/> Marketing <input type="checkbox"/> Manufacturing <input type="checkbox"/> Other (please write in) _____
		<input type="checkbox"/> Accounting <input type="checkbox"/> Sales <input type="checkbox"/> Information Systems <input type="checkbox"/> President/CEO <input type="checkbox"/> General Management
5	In which of the following areas of functional responsibility have you held an executive or managerial position? (check as many as appropriate)	<input type="checkbox"/> Engineering <input type="checkbox"/> Finance <input type="checkbox"/> Marketing <input type="checkbox"/> Manufacturing <input type="checkbox"/> Other (please write in) _____
		<input type="checkbox"/> Accounting <input type="checkbox"/> Sales <input type="checkbox"/> Information Systems <input type="checkbox"/> President/CEO <input type="checkbox"/> General Management
6	Your Age: _____	7. Gender <input type="checkbox"/> Male <input type="checkbox"/> Female
8	What is your highest level of education completed? (check only one)	<input type="checkbox"/> Attended high school <input type="checkbox"/> High school graduate <input type="checkbox"/> Attended college
		<input type="checkbox"/> College graduate <input type="checkbox"/> Attended graduate school <input type="checkbox"/> Obtained graduate degree
9	Do you have a college degree in (check as many as appropriate)	<input type="checkbox"/> Business <input type="checkbox"/> Bachelor _____ Year <input type="checkbox"/> Master _____ Year <input type="checkbox"/> Engineering <input type="checkbox"/> Bachelor _____ Year <input type="checkbox"/> Master _____ Year
		<input type="checkbox"/> Liberal Arts <input type="checkbox"/> Bachelor _____ Year <input type="checkbox"/> Master _____ Year <input type="checkbox"/> Other (please write in) _____ Year

THANK YOU FOR YOUR COOPERATION!

Approximately how long did it take you to complete this questionnaire? _____ minutes.

_____ This number is for analytical purposes only. Again, all responses will be held in strict confidence.

CENTER FOR INFORMATION
TECHNOLOGIES MANAGEMENT

THE UNIVERSITY OF TEXAS
AT ARLINGTON



SECURITY RISK MANAGEMENT
RESEARCH PROJECT

CHIEF INFORMATION OFFICIAL

THE PURPOSE OF THIS QUESTIONNAIRE IS TO OBTAIN INFORMATION ON COMPANY SECURITY RISK MANAGEMENT PROGRAMS. ALL INFORMATION WILL BE HELD IN STRICT CONFIDENCE, AS HAS ALWAYS BEEN THE POLICY OF THE UNIVERSITY OF TEXAS AT ARLINGTON WITH SPONSORED RESEARCH. WHEN THE RESULTS OF THIS STUDY ARE PUBLISHED, IT WILL BE IMPOSSIBLE TO IDENTIFY SPECIFIC INDIVIDUALS OR FIRMS.

WHEN YOU HAVE COMPLETED THE QUESTIONNAIRE, PLEASE SEAL IT IN THE ATTACHED ENVELOPE FOR MAILING TO THE LOCATION THAT WILL BE PROCESSING THE DATA.

THANK YOU FOR YOUR HELP.

RISK PROPENSITY

The following items ask about how your firm conducts business in its primary industry. (cio)

Always answer the question using a 1 to 7 scale by circling the correct digit unless otherwise noted.

Business Risk	Strongly agree						Strongly disagree
1 Our operation can be generally characterized as high risk.	1	2	3	4	5	6	7
2 We seem to adopt a rather conservative view when making major decisions.	1	2	3	4	5	6	7
3 New projects are approved on a "stage-by-stage" basis rather than with "blanket" approval.	1	2	3	4	5	6	7
4 We seem to have a tendency to support projects where the expected returns are certain.	1	2	3	4	5	6	7
5 Operations have generally followed the "tried and true" paths.	1	2	3	4	5	6	7

RISK PROPENSITY

The following items ask about how your firm handles the business risks associate with security in its primary industry (cio)

Always answer the question using a 1 to 7 scale by circling the correct digit unless otherwise noted.

Security Risk	To a large extent						Not at all	
1. We have protective security measures in place that are cost-effective and have reduced the level of risk to acceptable levels.	1	2	3	4	5	6	7	
2. The overall security philosophy at this location is to provide very tight security without hindering productivity.	1	2	3	4	5	6	7	
3. We have a risk acceptance program in order to allow managerial flexibility where the business reason justifies the security risk to the organization.	1	2	3	4	5	6	7	
4. We have insurance (separate policy or rider) specifically for computer security loses.	<input type="checkbox"/> Yes							<input type="checkbox"/> No
4a. If Yes, what is the annual premium cost of such insurance.	\$ _____							
5. We have a business recovery plan in place.	<input type="checkbox"/> Yes							<input type="checkbox"/> No

5a. If Yes, check off all that apply	<input type="checkbox"/> includes LAN recovery <input type="checkbox"/> includes telecommunications <input type="checkbox"/> includes mainframe	<input type="checkbox"/> includes a hot site contract <input type="checkbox"/> includes workgroup
6. If Yes, how recently was it tested?	<input type="checkbox"/> within the last 12 months <input type="checkbox"/> 1 to 2 years <input type="checkbox"/> more than 2 years	<input type="checkbox"/> never <input type="checkbox"/> don't know

IT RESOURCE POSTURE

The following items ask for your personal assessment about how your firm utilizes its Information Technology platform and its information resources. (cio)

Always answer the questions using a 1 to 7 scale by circling the correct digit unless otherwise noted.

Strategic Integration	To a large extent	Not at all
1 We offer computer-related products or services to our customers, distributors, or suppliers.	1 2 3 4 5 6 7	
2 We offer computer-related products or services to our competitors.	1 2 3 4 5 6 7	
3 We store information in our data bases which is accessed and used by our customers, distributors, or suppliers.	1 2 3 4 5 6 7	
4 Our computer resources help us build closer ties with other firms.	1 2 3 4 5 6 7	
5 Information systems technology helps us improve our products and services.	1 2 3 4 5 6 7	
6 We have computer applications which support our products.	1 2 3 4 5 6 7	
7 We have developed computer applications which are an integral part of our products.	1 2 3 4 5 6 7	
8 Our computer systems help direct and control production of our product and / or services.	1 2 3 4 5 6 7	
9 Much of the corporation's competitive position may depend on controlling the information it has.	1 2 3 4 5 6 7	

Electronic Integration (EI) Level	To a large extent	Not at all
1 Our computer systems exchange information with our customers/distributors (e.g. electronic payments, order entry, order-tracking).	1 2 3 4 5 6 7	
2 Our computer systems exchange information with our suppliers (e.g. electronic payments, order entry, order-tracking).	1 2 3 4 5 6 7	
3 Our computer systems provide inventory status and allow the initiation of an inventory release/build transaction by our customers /distributors.	1 2 3 4 5 6 7	
4 Our computer systems allow us to check inventory status and allow us to initiate an inventory release/build transaction with our suppliers.	1 2 3 4 5 6 7	
5 Our computer systems allow us to share business process information with business alliance organizations in order to improve efficiency and effectiveness amongst the group (e.g. design activities with manufacturing processes).	1 2 3 4 5 6 7	
6 Our computer systems allow us to share knowledge necessary to assess and interpret complex data (e.g. technical, managerial, legal, medical) with specific organizations.	1 2 3 4 5 6 7	
Reach And Range		
1 Whom can you easily reach? Please check off all that apply		
<input type="checkbox"/> Anyone, anywhere <input type="checkbox"/> Customers, suppliers with the same IT base as yours <input type="checkbox"/> Across different business units domestically <input type="checkbox"/> Within a single business unit location	<input type="checkbox"/> Customers, suppliers regardless of IT base <input type="checkbox"/> Across different business units abroad <input type="checkbox"/> Across geographically spread single business unit locations	
2 What services can you share automatically and seamlessly? Please check all that apply		
<input type="checkbox"/> Send messages, i.e. send a memo <input type="checkbox"/> Perform transactions [simple, i.e. take orders]	<input type="checkbox"/> Access to information, i.e. check credit rating <input type="checkbox"/> Perform transactions [complex on multiple applications, i.e. process orders]	

FIRM SIZE

Please answer the following questions about your firm's size and the application of Information Technology. (cio)

Number of Employees/Computer Users		
1	What is the total number of employees at this site (managerial, supervisory, line employees, etc.)?	
2	What is the total number of employees at this site that are computer users?	
3	What is the total number of external users that have access to the information resources of this firm? (Please provide estimates)	firms _____ customers _____ suppliers _____
Computer Resources		
1	Please check the categories that best describe the current computer resource deployment. (Check all that apply)	
<input type="checkbox"/>	A few unconnected PCs	<input type="checkbox"/> Unconnected minis and micros
<input type="checkbox"/>	Many networked minis and micros	<input type="checkbox"/> Many unconnected PCs
<input type="checkbox"/>	Many networked minis and micros, a mainframe and site LANs and WANs	<input type="checkbox"/> A company extranet
		<input type="checkbox"/> Several mainframes
		<input type="checkbox"/> Several unconnected PCs
		<input type="checkbox"/> A company Intranet
		<input type="checkbox"/> A mainframe
Finally we would like to ask you a few questions about your background. Again, all responses are confidential. (cio)		
1	How many years have you been employed by your present firm?	
2	How many years of work experience do you have in your present industry?	
3	How many years have you been in your present position in your company?	
4	What would you consider to be your primary functional responsibility at the present time? (check <u>one</u> only)	<input type="checkbox"/> Engineering <input type="checkbox"/> Finance <input type="checkbox"/> Marketing <input type="checkbox"/> Manufacturing <input type="checkbox"/> Other (please write in) _____
		<input type="checkbox"/> Accounting <input type="checkbox"/> Sales <input type="checkbox"/> Information Systems <input type="checkbox"/> President/CEO <input type="checkbox"/> General Management
5	In which of the following areas of functional responsibility have you held an executive or managerial position? (check as many as appropriate)	<input type="checkbox"/> Engineering <input type="checkbox"/> Finance <input type="checkbox"/> Marketing <input type="checkbox"/> Manufacturing <input type="checkbox"/> Other (please write in) _____
		<input type="checkbox"/> Accounting <input type="checkbox"/> Sales <input type="checkbox"/> Information Systems <input type="checkbox"/> President/CEO <input type="checkbox"/> General Management

6 Your Age: _____	7. Gender <input type="checkbox"/> Male <input type="checkbox"/> Female	
8 What is your highest level of education completed? (check only one)	<input type="checkbox"/> Attended high school <input type="checkbox"/> High school graduate <input type="checkbox"/> Attended college	<input type="checkbox"/> College graduate <input type="checkbox"/> Attended graduate school <input type="checkbox"/> Obtained graduate degree
9 Do you have a college degree in (check as many as appropriate)	<input type="checkbox"/> Business <input type="checkbox"/> Bachelor _____ Year <input type="checkbox"/> Master _____ Year <input type="checkbox"/> Engineering <input type="checkbox"/> Bachelor _____ Year <input type="checkbox"/> Master _____ Year	<input type="checkbox"/> Liberal Arts <input type="checkbox"/> Bachelor _____ Year <input type="checkbox"/> Master _____ Year <input type="checkbox"/> Other (please write in) _____ Year

THANK YOU FOR YOUR COOPERATION!

Approximately how long did it take you to complete this questionnaire? _____ minutes.

_____ This number is for analytical purposes only. Again, all responses will be held in strict confidence.

SECURITY RISK MANAGEMENT RESEARCH PROJECT

PLEASE CHECK OFF ALL THAT APPLY

Our organization declined to take part in the research study for the following reason(s)

1. The organization does not accept unsolicited submissions of any ideas or materials	
2. The request did not comply with our established policies for survey requests.	
3. Due to the large volume of survey requests we receive our policy is not to participate in any surveys	
4. Due to the large volume of survey requests we receive we cannot participate in every one we receive	
5. The corporate headquarters is responsible for such decisions and the survey was forwarded there	
6. Temporary issues (company being sold/reorganization is in progress)	
7. The university sponsor for the research study cannot provide legal confidentiality protection	
8. The use of individual identification numbers on the questionnaires could be used to reveal responses by an individual or by the organization	
9. The questionnaires contain some questions that require answers that would reveal proprietary information	
10. The questionnaires contain many questions that would require checking company records	
11. We do not share any information about our computer security policies with outside entities	
12. Our management team is too busy to spend time filling out any survey questionnaires	

13. The time of our management team is valuable and we decided that the benefits we would receive for the time expended was not adequate to participate in the research project.	
14. Company security policies prevent complete answers to some of the requested information	
15. Company policy prevents revealing any demographic information about our management team	
16. Company policy prevents revealing any information about our management team business philosophy or internal actions	
17. OTHER:	

I appreciate the time you took to furnish me feedback as to the reason(s) why your organization chose not to participate in the research study.

Thank You
Andrew G. Kotulic

APPENDIX B
RESEARCH STUDY LETTERS

PRACTICE SAFE COMPUTING

0000

Mr. Davie Subject
The Corp
Po Box XXXX
AnyTown USA 00000

Subject: Effective Security Risk Management Programs

Dear Mr. Subject

My name is Andrew G. Kotulic, Assistant Professor Information Systems-York College of Pennsylvania. I am soliciting your support for the first known research study that attempts to identify organizational factors that contribute to the effectiveness of Security Risk Management (SRM) programs. The sponsor is **The Center for Information Technologies Management-The University of Texas at Arlington.**

Research Study Scope

The sample population consists of 1500 major corporations from a wide range of business sectors. The research study requires the responses from four individuals at each organization. The questionnaires for the CIO, other TMT member and functional manager should not take more than 10-20 minutes to answer. The questionnaire for the CSO is more extensive and will take 20-30 minutes to answer.

The support of top management is crucial for the accomplishment of the planned goals for this study. The published results of the research study could aid your management team during their security policy decision making process.

A leading firm in the security industry has evaluated the questionnaires. The firm concluded that answers to the questions could not lead to the compromise of computer security at an organization. Additionally, nothing that would reveal firm identity or individuals in the firm will appear in the published results of the study.

I have included the following items with this letter:

(A) Separate questionnaires for a member of the top management team (TMT), the highest-level security official (CSO), the highest ranking information official (CIO), and a functional level manager.

PRACTICE SAFE COMPUTING

(B) Four postage paid envelopes for the individual respondents to return their questionnaires directly to me.

(C) A token of my gratitude for you and for each of the individuals selected to fill out the questionnaires.

Respectfully,

Andrew G. Kotulic
Assistant Professor Information Systems

P.S. I will appreciate your help to insure that your firm is included in the research study. If there are any questions or comments, please feel free to have someone contact me at 717.815.1411 or by e-mail at agkotulic@eagle.ycp.edu. Additionally, I will furnish a copy of the summary results to each firm that returns the four completed questionnaires.

PRACTICE SAFE COMPUTING

0000

Ms. Mary Conway
Hands On Industries
36 Western Street
Any Place USA 00000

Subject: Research Study-Effective Security Risk Management Programs

Dear Ms. Conway

I recently sent you a request soliciting your support for a research study that attempts to identify organizational factors that contribute to the effectiveness of Security Risk Management (SRM) programs.

I understand that some organizations are reluctant to release any information about their computer security programs. Additionally, I realize that due to today's business environment requests for any management time must be evaluated based on what benefits will result from the efforts expended.

Several firms that have returned the four completed questionnaires have requested that I provide them a profile of their organization relative to other firms. They felt that receiving a summary of the results would not be totally beneficial. **Therefore, I will provide firms that return the four completed questionnaires an executive summary that can be used to evaluate firm level organizational characteristics relative to the total population. The final product will depend on the response rate by SIC. Additionally, I will have to consider different options so that individual responses would not be revealed in the executive summary. I want to emphasize that firm and individual identity will not be revealed and that as soon as I send out the executive summary report to an organization all information that could link an organization to the responses will be destroyed.**

I would appreciate your firm taking part in the research study since the larger the response rate the more beneficial the published findings will be for business organizations. If the original questionnaires have been disposed of and your firm is interested in receiving this type of firm level executive summary, I would appreciate being contacted via e-mail at agkotulic@eagle.ycp.edu. I would immediately send out a duplicate set of the four questionnaires. Additionally, if you still choose not to take part in the research study I would appreciate your feedback as to the reason(s) why your organization chose not to participate in the study. This area is my main research interest and any information you could furnish me will help me in planning future studies.

PRACTICE SAFE COMPUTING

I have included a check list of major reasons organizations have decided not to take part in research studies. This form can be used for your feedback and returned to me via the postage paid envelope or you could have someone furnish me your feedback via e-mail.

Respectfully,

Andrew G. Kotulic
Assistant Professor Information Systems

REFERENCES

- Abrams, M. D., & Moffett, J. D. (1995). A higher level of computer security through active policies. Computers and Security, 14, 147-157.
- Abrams, M. D., & Toth, P. R. (Eds.). (1994). Proceedings of an invitational workshop on information technology (IT) assurance and trustworthiness, March 21-23. Williamsburg, VA: Aerospace Computer Security Associates (ACSA).
- Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behavior. Englewood Cliffs, NJ: Prentice Hall.
- Anderson, H. (1997). Securing your intranet: Minimizing the risk of interconnectivity. PC Today: Online Report. Retrieved from the World Wide Web January, 1997. [Http://www.pc-today.com/editorial/goingonline/960836sm.html](http://www.pc-today.com/editorial/goingonline/960836sm.html)
- Andrews, K. A. (1980). The concept of corporate strategy (rev.). New York: Dow-Jones.
- Ansoff, H. I. (1965). Corporate strategy. New York: McGraw-Hill
- Applegate, L. M., & Elam, J. J. (1992). New information systems leaders: A changing role in a changing world. MIS Quarterly, 16, 469-489.
- Astley, W. G., & Formbrum, C. J. (1983). Collective strategy: The social ecology of organizational environments. Academy of Management Review, 8(4), 576-587.
- Axelrod, C. W. (1990). Security during system recovery and repair. Journal of Information Systems Management, 7(1), 42-47.
- Banham, R. (1995). The convergence of risk. Risk Management, 42(7), 22-28.
- Barnes, C. C., & Harris, W. T. (1990). A survey of microcomputer security at AACSB universities. INTERFACE, 12(2), 13-15.

Baroudi, J. L., & Orlikowski, W. J. (1989). The problem of statistical power in MIS research. MIS Quarterly, 13(1), 87-106.

Barton, S. L., & Gordon, P. J. (1987). Corporate strategy: Useful perspective for the study of capital structure? Academy of Management Review, 12(1), 67-75.

Baskerville, R. (1988). Designing information systems security. New York: John Wiley.

Baskerville, R. (1992). The developmental duality of information security. Journal of Management Systems, 4(1), 1-12.

Baskerville, R., & Smithson, S. (1995). Information technology and new organizational forms: Choosing chaos over panaceas. European Journal of Information Systems: An Official Journal of the Operations Research Society, 4(2), 66-73.

Bates, W. S. (1970). Security of computer-based information systems. Datamation, 16(5), 60-65.

Bearden, W. O., & Teel, J. E. (1983). Selected determinates of consumer satisfaction and complaint reports. Journal of Marketing Research, 20, 21-28.

Benjamin, R. I., De Long, D. W., & Scott-Morton, M. S. (1990). Electronic data interchange: How much competitive advantage? Long Range Planning, 23(1), 29-40.

Bennett, S. P., & Kailay, M. P. (1992). An application of qualitative risk analysis to computer security for the commercial sector. Proceedings of the 8th. Annual Computer Security Applications Conference. IEEE Press. 64-73.

Bergeron, F., & Berube, C. (1990). End users talk computer policy. Journal of Systems Management, 41(12), 14-32.

Bidgoli, H; & Azarmsa, R. (1989). Computer security: New managerial concern for the 1980s and beyond. Journal of Systems Management, 40(10), 21-27.

- Blackhouse, J., & Dhillon, G. (1995). Managing computer crime: A research outlook. Computers and Security, 14, 645-651.
- Blough, K. (1999, November). In search of more-secure extranets. InformationWeek, 1. Download from the Web Site. [Http://www.informationweek.com/759/extranet.htm](http://www.informationweek.com/759/extranet.htm)
- Bodeau, D. J. (1992). A conceptual model for computer risk analysis. Proceedings of the 8th. Annual Computer Security Applications Conference. IEEE Press, 56-63.
- Boockholdt, J. L. (1989). Implementing security and integrity in micro-mainframe networks. MIS Quarterly, 13(2),135-144.
- Borcherding, K., Rohramann, B., & Eppel, T. (1986). A psychological study on the cognitive structure of risk evaluations. In B. Brehmer, H. Junger-Mann, P. Lourens, & G. Sevon (Eds.), New directions in research on decision making (pp. 245-162). Amsterdam: North-Holland.
- Bourgeois, L. J. (1980). Strategy and environment: A conceptual integration. Academy of Management Review, 5(1), 25-39.
- Bourgeois, L. J. (1985). Strategic goals, perceived uncertainty, and economic performance in volatile environments. Academy of Management Journal, 28, 548-573.
- Bovass, G. (1992). A structural analysis of the formation of a network organization. Group and Organizational Management, 17(1), 86-106.
- Brancheau, J. C., & Wetherbe, J. C. (1987). Key issues in information systems management. MIS Quarterly, 11(1), 23-45.
- Briney, A. (2000). Security focused: 2000 industry survey. Information Security, 3(9), 40-68.
- Broadbent, M., Weill, P., O'Brien T., & Neo, B. S. (1996). Firm context and patterns of IT infrastructue capability. Proceedings of the 17th International Conference on Information Systems, December 16-18, 1996. Cleveland, OH, 174, 194.

Bruno, L. (1999). Intranets soar but security hurdles remain. Released by TechWeb: 19 July 1999. Retrieved from [Http://www.techweb.com/wire/story/TWB19990719S0002](http://www.techweb.com/wire/story/TWB19990719S0002)

Burns, T., & Stalker, G. M. (1961). The management of innovation. London: Tavistock.

Burt, R. S., & Celotto, N. (1992). The network structure of management roles in a large matrix firm. Evaluation and Program Planning, 15, 303-326.

Byrne, J. A. (1993, February 8). The virtual corporation. Business Week, pp. 98-103.

Byrne, J. A. (1993a, December 20). The horizontal corporation. Business Week, pp. 76-81.

Byrd, T. A., Sambamurthy, V., & Zmud, R. W. (1995). An examination of IT planning in a large, diversified public organization. Decision Sciences, 26(1), 49-73.

Carmines, E. G., & Zeller, R. A. (1979). Reliability and validity assessment. In J. Sullivan (Ed.), Quantitative applications in the social sciences series. Newbury Park, CA: Sage.

Cash, J. I., McFarlan, F. W., McKenney, J. L., & Applegate, L.M. (1992). Corporate information systems management: Text and cases (3rd ed.). Irwin.

Cassidy, P. (1994). Data integrity: Lines of defense. CIO, 7(9), 46-54.

Castrogiovanni, F. (1991). Environmental munificence: A theoretical assessment. Academy of Management Review, 16, 542-565.

Ceraolo, J. (1996). Penetration testing through social engineering. Information Systems Security, 4: 37+. Downloaded Retrieved November , 1996, from Electric Library database (Infonautics Corporation) on the World Wide Web: <http://www.infonautics.com>.

Chakravarthy, B. S., & Doz, Y. (1992). Strategy process research: Focusing on corporate self-renewal. Strategic Management Journal, 13, 5-14.

Chan, Y. E. (1992). Business strategy, information systems strategy, and strategic fit: Measurement and performance impacts. Unpublished dissertation, The University of Western Ontario.

Chan, Y. E., & Huff, S. L. (1994). The development of instruments to assess information systems and business unit strategy and performance. In N. Venkatraman & John Henderson (Eds.), Research in strategic management and information technology (Vol. 1). Greenwich, CT: JAI Press.

Charan, R. (1991). How networks reshape organizations for results. Harvard Business Review, 69(5), 104-115.

Checkland, P. (1981). Systems thinking, systems practice. Chichester: John Wiley.

Checkland, P., & Scholes, J. (1990). Soft systems methodology in action. Chichester: John Wiley.

Child, J. (1973). Strategies of control and organizational behavior. Administrative Science Quarterly, 18, 1-17.

Christine, B. (1995). Computers under the hack attack. Risk Management, 42(3), 49.

Churchill, G. A. (1979). A paradigm for developing better measures of marketing constructs. Journal of Marketing Research, 16(1), 64-73.

Churchill, G. A., & Surprenant, C. (1982). An investigation into the determinants of customer satisfaction. Journal of Marketing Research, 19(4), 491-504.

Cobb, S. (1996). Internet firewalls: The demand for good internet firewalls is spurred by the growing number of intrusion incidents. Retrieved from The National Computer Security Association (NCSA) home page which is now TrueSecure Corporation. [Date Unknown].<http://truesecure.com>.

Cohen, J. (1977). Statistical power analysis for the behavioral sciences (rev.). New York: Academic.

Cohen, M. D. (1991). Individual learning and organizational routine: Emerging connections. Organization Science, 2(1), 135-139.

Cortese, A. (1996, February 26). Here comes the intranet cover story. Business Week. Downloaded from the WWW. October, 1996. <http://www.businessweek.com/1996/09/b34641.htm>.

Covin, J. G., & Slevan, D. P. (1988). The influence of organization structure on the utility of an entrepreneurial top management style. Journal of Management Studies, 23(3), 217-234.

Covin, J. G., & Slevin, D. P. (1989). Strategic management of small firms in hostile and benign environments. Strategic Management Journal, 10(1), 75-87.

Cronbach, L. (1951). Coefficient alpha and the internal structure of tests. Psychometrika 16(3), 297-335.

Cronbach, L. J., & Meehl, P. E. (1971). Construct validity in psychological tests. Psychological Bulletin, 52, 281-302.

Cyert, R. M., & March, J. G. (1963). A behavioral theory of the firm. Englewood Cliffs, NJ: Prentice-Hall.

Daft, R. L., & Lewin, A. Y. (1993). Where are the theories for the "new" organizational forms? An editorial essay. Organization Science, 4(4), i-vi.

Daft, R. L., Sormunen, J., & Parks, D. (1988). Chief executive scanning, environmental characteristics, and company performance: An empirical study. Strategic Management Journal, 9, 123-129.

Daft, R. L., & Weick, K. E. (1984). Toward a model of organizations as interpretation systems. Academy of Management Review, 9, 284-295.

Dalton, G. (1998, August 31). Acceptable risks. InformationWeek, pp. 36-48.

Damanpour, F. (1991). Organizational innovation: A meta-analysis of effects of determinants and Moderators. Academy of Management Journal, 34(3), 555-590.

Daniels, C. (1991). The management challenge of information technology. Special Report No. 2125. London: The Economist Intelligence Unit Limited & Business International.

Davidson, W. H. (1993). Beyond re-engineering: The three phases of business transformation. IBM Systems Journal, 32(1), 65-79.

Davies, D. W., & Price, W. L. (1984). Security for computer networks: An introduction to data security in teleprocessing and electronic funds transfer. New York: John Wiley.

Dean, E. B. (1996). Risk: From the perspective of competitive advantage. Retrieved from World Wide Web. July, 1996. [Http://dfac.larc.nasa.gov/dfc/rsk.html](http://dfac.larc.nasa.gov/dfc/rsk.html)

DeLone, W. H. (1988). Determinants of success of computer usage in small business. MIS Quarterly, 12(1), 51-61.

DeLone, W. H., & McLean, E. R. (1992). Information Systems Success: The Quest for the Dependent Variable. Information Systems Research, 3(1), 60-95.

DeLong, D. F. (2001). Hackers said to cost U.S. billions. NewsFactor Network. February 8 issue. Retrieved February 12, 2001, from the World Wide Web: <http://www.econnercetimes.com/perl/printer/7349>

DeMaio, H. B. (1995) Information protection and business process reengineering. Information Systems Security. 3: pp. 5+ Retrieved from Electric Library-Infonautics Corporation January, 1996.

DeMaio, H. B. (1995a). Open systems security and the art of random juggling. Information Systems Security, 4: pp 7+ Retrieved from Electric Library-Infonautics Corporation March, 1996

Dess, G. G., Ireland. D. R., & Hitt, M. A. (1990). Industry effects and strategic management research. Journal of Management, 16(1), 5-25.

Dess, G. G., & Origer, N. K. (1987). Environment, structure and consensus in strategy formulation: A conceptual integration. Academy of Management Review, 12, 313-330

Dess, G. G., Rasheed, M. A., McLaughlin, K. J., & Priem, R. L. (1995). The new corporate architecture. Academy of Management Executive, 9(3), 7-20.

Devanna, M. A., & Tichy, N. (1990). Creating the competitive organization of the 21st century: The boundaryless corporation. Human Resource Management, 23(4), 455-471.

Dillman, D. A. (1978). Mail and telephone surveys: The total design method. New York: Wiley-Interscience.

Dillman, D. A. (2000). Mail and internet surveys: The tailored design method (2nd ed.). New York: John Wiley.

Doty, D. H., Glick, W. H., & Huber, G. P. (1993). Fit, equifinality, and organizational effectiveness: A test of two configurational theories. Academy of Management Journal, 36, 1196-1250.

Doty, T. (1995). Test driving SATAN. Computer Security Journal, 11(2), 9-14.

Doz, Y. L., & Prahalad, C. K. (1991). Managing DMNCs: A search for a new paradigm. Strategic Management Journal, 12, 145-164.

Duncan, R. B. (1972). Characteristics of organizational environments and perceived environmental uncertainty. Administrative Science Quarterly, 17, 313-327.

Duncan, R. B. (1979). What is the right organizational structure? Decision tree analysis provides the answer. Organizational Dynamics, 7, 59-80.

Edupage (1996) CERT for a fee. Edupage (1996, 26 May 26) Edupage Editors from Information Week, 20 May 96, p. 32.

Edupage (1996a). U.S. official warns of "Electronic Pearl Harbor" Edupage (1996a, July 21). Edupage Editors from BNA Daily Report for Executives 17 Jul 96 A22.

Edwards, J. (1994). Be prepared. CIO, 7(11), 68-72.

Ein-Dor, P., & Segev, E. (1978). Organizational context and the success of management information system. Management Science, 24(10), 1067-1077.

Eisenhardt, K. M. (1989a). Building theories from case study research. Academy of Management Review, 14(4), 532-555.

Eisenhardt, K. M. (1989b). Making fast strategic decisions in high-velocity environments. Academy of Management Journal, 12(3), 543-576.

Eisenhardt K. M. (1991). Better stories and better constructs: The case for rigor and comparative logic. Academy of Management Review, 16(3), 620-627.

Eisenhardt, K. M., & Bourgeois, L. J. (1988). Politics of strategic decision making in high velocity environments: Toward a midrange theory. Academy of Management Journal, 31(4), 737-770.

Eloff, J. H. P., Labuschagne, L., & Badenhorst, K. P. (1993). A comparative framework for risk analysis methods. Computers and Security, 12, 597-603.

Enger, N. L., & Howerton, P. W. (1980). Computer security. A management audit approach. New York: AMACOM: A Division of American Management Associations.

Fagan, P. (1993). Organizational issues in IT security. Computers and Security, 12, 710-715.

Farmer, T. A. (1993). Testing the effect of risk attitude on auditor judgements using multiattribute utility theory. Journal of Accounting, Auditing & Finance, 8(1), 91-110.

Fialka, J. J. (1996). 6 June, 1996, Wall Street Journal Interactive Edition. John J. Fialka, Staff reporter of the Wall Street Journal. <http://public.wsj.com/home.html>

Fine, N. (1995). Competitive intelligence: An external threat and an internal requirement. Computer Security Journal, 11(2), 75-78.

Fischhoff, B., Lichtenstein, S., Slovic, P., Derby, S. L., & Keeney, R; (1981). Acceptable risk. New York: Cambridge University Press.

Fischhoff, B., Slovic, P., Lichtenstein, S. Read S., & Combs, B. (1978). How safe is safe? A psychometric study of attitudes towards technological risks and benefits. Policy Science, 9, 127-152.

Fisher, R. P. (1984). Information systems security. Englewood Cliffs, NJ: Prentice-Hall

Forcht, K. A. (1994). Computer security management. Danvers, MA: Boyd & Fraser.

Frank, J. (1988). Quality control of personnel computing. Journal of Systems Management, 39(12), 32-39.

Fredrickson, J. W. (1984). The comprehensiveness of strategic decision processes: Extension, observations, future directions. Academy of Management Journal, 27(3), 445-466.

Fried, L. (1993). Distributed information security: Responsibility assignments and costs. Information Systems Management, 10, 56-65.

Fried, L. (1994). Information security and new technology. Information Systems Management, 11(3), 57-63.

Froot, K. A., Scharfstein, D. S., & Stein, J. C. (1994). A framework for risk management. Harvard Business Review, 91-102.

Galbraith, J. R. (1974). Organization design: An information processing view. Interfaces, 4(3), 28-36.

Galbraith, J. R., & Kazanjian, R. (1986). Strategy Implementation: Structure, systems, and process (2nd ed.). St. Paul, MN: West Publishing.

GAO (1996a). Information security: Computer attacks at Department of Defense pose increasing risks. Report Number AIMD-96-84 (05/22/96).

Glazer, R. (1993). Measuring the value of information: The information-intensive organization. IBM Systems Journal, 32(1), 99-110.

Goodhue, D. L., & Straub, D. W. (1991). Security concerns of system users: A study of perceptions of the adequacy of security. Information and Management, 20, 13-27.

Grant, B. (1992). Controlling the data resource in an expanding business environment. Data Resource Management, 3(2), 22-27.

Hage, J. (1988). The pathways of evolution in organizations. In J. Hage (Ed.), Futures of organizations: Innovating to adapt strategy and human resources to rapid technological change (pp. 44-65). Lexington, MA: Lexington Books.

Haines, Y. Y. (1991). Editorial: Total risk management. Risk Analysis, 11(2), 169-171.

Hambrick, D. C. (1983). An empirical typology of mature industrial-product environments. Academy of Management Journal, 26(2), 213-230.

Hambrick, D. C. (1987). The top management team: Key to strategic success. California Management Review, 30(1), 88-108.

Hambrick, D. C., & Mason, P. A. (1984). Upper echelons: The organization as a reflection of its top managers. Academy of Management Review, 9(2), 193-206.

Hamilton, C. R. (1995). Case study: Automated risk analysis. Computer Security Journal, 11(1), 35-42.

Hamilton, P. (1973). Computer security (1st ed.). Philadelphia, PA: AUERBACH.

Hannan, M. T., & Freeman, J. (1984). Structural inertia and organizational change. American Sociological Review, 49, 149-164.

Hart, S. (1992). An integrative framework for strategy-making processes. Academy of Management Review, 17, 327-351.

Hatten, K. J., Schendel, D. E., & Cooper, A. C. (1978). A strategic model of the U.S. brewing industry: 1952-1971. Academy of Management Journal, 21(4), 592-610.

Henderson, J. C., & Venkatraman, N. (1992). Strategic alignment: A model for organizational transformation via information technology. In T. A. Kochan & M. Useem (Eds.), Transforming organizations. Oxford: Oxford University Press.

Henderson, J. C., & Venkatraman, N. (1993). Strategic alignment: Leveraging information technology for transforming organizations. IBM Systems Journal, 32(1), 4-16.

Herold, R. (1994). Case study: An information security program. Computer Security Journal, 10(2), 17-26

Highland, H. J. (1992). The security impact of networks, telecommunications, and office automation. Computers and Security, 11, 227-232.

Highland, H. J. (1993). A view of information security tomorrow. Computers and Security, 12, 634-639.

Hill, S., & Smith, M. (1995). Risk management and corporate security: A viable leadership and business solution designed to enhance corporations in the emerging marketplace. Computers and Security, 14, 199-204.

Hitchings, J. (1995). Deficiencies of the traditional approach to information security and the requirements for a new methodology. Computers and Security, 14, 377-383.

Ho, S. S. M. (1992). The impact of using risk analysis in capital budgeting on earnings performance: The UK experience. The International Journal of Accounting, 27(1), 1-14.

Holtgrave, D. R., & Weber, E. U. (1993). Dimensions of risk perception for financial and health risks. Risk Analysis, 13(5), 553-558.

Hoppe, N. (1994). Achieving consistent security controls throughout a multinational organization. Computers and Security, 13(1), 23-29.

Huber, G. P. (1982). Organizational information systems: Determinants of their performance and behavior. Management Science, 28(2), 138-155.

Huber, G. P. (1991). Organizational learning: An examination of the contributing processes and a review of the literatures. Organization Science, 2(1), 88-115.

Huber, G. P., & Daft R. L. (1987). The information environments of organizations. In F. M. Jablin, L. L. Putman, K. H. Roberts, & L. W. Porter (Eds.), Handbook of organizational communication: An interdisciplinary perspective (pp. 130-164). Beverly Hills, CA: Sage.

Huff, A. S., & Reger, R. K. (1987). A review of strategic process research. Journal of Management, 13(2), 211-236.

Hume, G. V. (2000). Vulnerabilities beckon some with a license to hack. Information Week (23, October, 2000). Retrieved January 2001, from InformationWeek.com on the World Wide Web: <http://www.informationweek.com/809/hacking.htm>

Information Security: Computer attacks at Department of Defense pose increasing risks (1996) AIMD-96-84 (05/22/96). Retrieved September 2000, Government Printing Office Web Site. <http://frwebgate3.access.gpo.gov>

INFOSYS—The Electronic Newsletter for Information Systems. (1996, June 22). Copy Editor, 3(18).

James, W. L., & Hatten, K. J. (1995). Further evidence on the validity of the self typing paragraph approach: Miles and Snow strategic archetypes in banking. Strategic Management Journal, 16(2), 161-168.

Jarvenpaa, S. L., & Ives, B; (1991). Executive involvement and participation in the management of information technology. MIS Quarterly, 15(2), 205-227.

Jarvenpaa, S. L., & Ives, B. (1994). Organizational fit and flexibility: IT design principals for a globally competing firm. In N. Venkatraman & John Henderson (Eds), Research in strategic management and information technology (Vol. 1). Greenwich, CT: JAI Press.

Johnston, H., & Vitale, M. (1988). Creating competitive advantage with organizational systems. MIS Quarterly, June, 153-165.

Jones, M. C., Arnett, K. P., Tang, J. E. (1993). Perceptions of computer viruses: A cross-cultural assessment. Computers and Security, 12, 191-197.

Joseph, G. W. (1990). Computer virus prevention and detection planning, Journal of Accounting and EDP, 5(4), 4-6.

Kabay, M. E. (1993). Social psychology and INFOSEC: Psycho-social factors in the implementation of information security policy. NCSA home page.

Kabay, M. E., & Walsh, L. M. (2000). 2000 year-in-review: The year in computer crime. Information Security, 3(12), 28-34.

Kahneman, L. R., Slovic, P., & Tversky, A. (Eds.). (1982). Judgment under uncertainty: Heuristics and biases (pp. 509-520). New York: Cambridge University Press.

Kahneman, L. R., & Tversky, A. (1982). Variants of uncertainty. Cognition, 11, 143-157.

Kailey, M. P., & Jarratt, P. (1995). RAMeX: A prototype expert system for computer risk analysis and management. 14, 449-463.

Kappelman, L. A. (1995). Measuring user involvement: A diffusion of innovation perspective. DATA BASE for Advances in Information Systems, 26(2/3), 65-86.

Kay, R. (1994). Distributed and secure. BYTE, 19(6), 165-178.

Keen, P. G. W. (1991). Shaping the future: Business design through information technology. Boston, MA: Harvard Business School Press..

Keen, P. G. W., & Cummins, J. M. (1994). Networks in action: Business choices and telecommunications decisions. Belmont, CA: Wadsworth.

Keeney, R., & Raiffa, H. (1976). Decisions with multiple objectives: Preferences and value tradeoffs. New York: John Wiley.

Kendall, W. R., & Scott, C. R. (1990). Protecting and classifying an important productive asset: Information! Information Age, 12(4), 195-198.

Kerlinger, F. (1973). Foundations of behavioral research. New York: Holt, Rinehart & Winston.

Kim, J. O., & Mueller, C. W. (1978). Factor analysis: Statistical methods and practical issues. Sage Series, #14. Beverly Hills, CA: Sage.

Kim, Y., & Kim, Y. (1999). Critical IS issues in the network era. Information Resources Management Journal, 12(4), 14-23.

King, W. (1995). Creating internal markets. Information Systems Management, 12, 61+. Retrieved September, 1996, from Electric Library database Infonautics Corporation on the World Wide Web: <http://www.infonautics.com>.

Koberg, C. S., Tegarden L., & Wilsted, W. (1993). Environmental and structural influences on the strategy making process of banks. Journal of Applied Business Research.

Konsynski, B. R. (1993). Strategic control in the extended enterprise. IBM Systems Journal, 32(1), 111-142.

Kramer, K. L., & Dutton, W. H. (Eds.). (1991) Survey research in the study of information systems. The information systems research challenge: Survey research methods (Vol. 3). Boston, MA: Harvard Business School Research Colloquium.

Kruys, J. P. (1991). Progress in secure distributed systems. Computers and Security, 10(5), 429-441.

LaBarbera, P.A., & Mazursky, D. (1983). A longitudinal assessment of consumer satisfaction/dissatisfaction: The dynamic aspect of the cognitive process. Journal of Marketing Research, 20, 393-404.

Lamkin, K.B., & Courtney, J. F. (1995). The role of schema and available information in individual decision-making tasks: An empirical study of locally rational decision-making.

1995 AIS American Conference, Downloaded off of the WWW, August, 1997.

[Http://hsb.baylor.edu/ramsower/acis/papers/lamkin.htm](http://hsb.baylor.edu/ramsower/acis/papers/lamkin.htm)

Lathrop, D. L. (1992). Security aspects of wireless local area networks. Computers and Security, 119(5), 421-426.

Lawrence, P. R., & Davis, S. (1978). Matrix. Readings, MA: Addison-Wesley.

Lawrance, W. W. (1976). Of acceptable risk. Los Altos, CA: William Kaufman.

Leonard-Barton, D., & Deschamps, I. (1988). Managerial influence in the implementation of new technology. Management Science, 34(10), 1252-1265.

Lewin, A. Y., & Stephens, C. U. (1994). CEO attitudes as determinants of organization design: An integrated model. Organization Studies, 15(2), 183-212.

Lichtenstein, S. (1996, March). Information security principals: A holistic view. Working Paper, Department of Information Systems, Monash University, Melbourne.

Lichtenstein, S., Slovic, P., Fischhoff, B., Layman, M., & Combs, B. (1978). Judged frequency of lethal events. Journal of Experimental Psychology: Human Learning and Memory, 4, 551-78.

Lightle, S., & Sprohge, H. (1992). Strategic information system risk. Internal Auditing, 8(1), 31-36.

Lim, S. B., & Jamieson, R. (1995). EDI risks, security and control: An Australian survey. Proceedings of AIS American Conference on Information Systems (pp. 1-6+), August 25-27, Pittsburg, PA. Retrieved 1996, from [Http://hsb.baylor.edu/ramsower/acis/papers/jamieso2.htm](http://hsb.baylor.edu/ramsower/acis/papers/jamieso2.htm)

Lindley, D. V. (1973). Making decisions. London: John Wiley.

Lindup, K. R. (1995). A new model for information security policies. Computers and Security, 14, 691-695.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. MIS Quarterly, 16(2), 173-186.

Lorange, P., & Roos, J. (1991). Why some strategic alliances succeed and others fail. Journal of Business Strategy, 12(1), 25-30.

MacCrimmon, K. R., & Wehrung, D. A. (1986). Taking risks: The management of uncertainty. New York: Free Press.

MacCrimmon, K. R., & Wehrung, D. A. (1990). Characteristics of risk taking executives. Management Science, 36(4), 422-435.

Madnick, S. E. (1991). The information technology platform (pp. 27-60). In E. Michael & S. Scott Morton (Eds.), The corporation of the 1990s: Information technology and organizational transformation. New York: Oxford University Press.

Madsen, W. (1995). Globalization of services: GATT, NAFTA, and the threat to information security. Information Systems Security, 4, 13+ Retrieved September 1996, from Electric Library database Infonautics Corporation) on the World Wide Web: <http://www.infonautics.com>.

Maharik, M., & Fischhoff, B. (1993). Risk knowledge and risk attitudes regarding nuclear energy sources in space. Risk Analysis, 13(3), 345-353.

March, J. G., & Shapira, Z. (1987). Managerial perspectives on risk and risk taking. Management Science, 33(11), 1404-1418.

March J., & Simon, H. (1958). Organizations. New York: John Wiley.

McDade, D. L. (1990). The assessment of perceived environmental uncertainty and economic performance. Human Relations, 43, 1203-1218.

McDaniels, T., Axelrod, L. J., & Slovic, P. (1995). Characterizing perception of ecological risk. Risk Analysis, 15(5), 575-588.

McDonald, T. (2000). Report: Year's hack attacks to cost \$1.6 trillion. E-Commerce Times. (11 July 2001). Retrieved February 2001, from the World Wide Web: <http://www.ecommercetimes.com/perl/printer/3741>

McGhie, L. (1994). A model for a secure distributed computing environment. Computer Security Journal, 10(2), 27-36.

McGaughey, R. E., Snyder, C. A., & Carr, H. H. (1994). Implementing information technology for competitive advantage: Risk management issues. Information and Management, 26(5), 273-280.

McGrath, J. E. (1982). Dilemmatics: The study of research choices and dilemmas. In J. E. McGrath, J. Martin & R. A. Kulka (Eds.), Judgement calls in research. Beverly Hills, CA: Sage.

McKim, R. A. (1992). Risk management-back to basics. Cost Engineering, 34(12), 7-12.

Mead, P. (1993). Taking the risk out of disaster recovery services. Risk Management, 40(1), 20-26.

Menkus, B. (1992). Concerns in computer security. Computers and Security, 11, 211-215.

Merkhofer, M. L., & Keeney, R. L. (1987). A Multi-attribute Utility analysis of alternative sites for the disposal of nuclear waste. Risk Analysis, 7, 173-194.

Merten, A. G., & Severance, D. G. (1981). Data processing control: A state-of-the-art survey of attitudes and concerns of DP executives. MIS Quarterly, 5(2), 11-32.

Metcalf, M., & Powell, P. (1995). Information: A perceiver-concerns perspective. European Journal of Information Systems: An Official Journal of the Operations Research Society, 4(3), 121-129.

Meyer, A. D., Tsui A. D., & Hinings, C. R. (1993). Configurational approaches to organizational analysis. Academy of Management Review, 36(6), 1175-1195

Miles, R. E., & Snow, C. C. (1995). The new network firm: A spherical structure built on a human investment philosophy. Organizational Dynamics, 23, 5+. Retrieved September, 1996, from Electric Library database (Infonautics Corporation) on the World Wide Web: <http://www.infonautics.com>

Miles, R. E., Snow, C. C., Meyer, A. D., & Coleman, H. J. (1978). Organizational Strategy, Structure, and Process. Academy of Management Review, 3(3), 546-562.

Miller, D. (1986). Configurations of strategy and structure: Towards a synthesis. Strategic Management Journal, 7(3), 233-249.

Miller, D. (1987). The genesis of configuration. Academy of Management Review, 12, 686-701.

Miller, D. (1987b). The structural and environmental correlates of business strategy. Strategic Management Journal, 8(1), 55-76.

Miller, D. (1987c). Strategy making and structure: Analysis and implications for performance. Academy of Management Journal, 30(1), 7-32.

Miller, D. (1992). Environmental fit versus internal fit. Organization Science, 3(2), 159-178.

Miller, D., Droge, C., & Toulouse, J. (1988). Strategic process and content as mediators between organizational context and structure. Academy of Management Journal, 31(3), 544-569.

- Miller, D., & Friesen, P. H. (1980). Archetypes of organizational transaction. Administrative Science Quarterly, 25(2), 268-299.
- Miller, D., & Friesen, P. H. (1983). Strategy making and environment: The third link. Strategic Management Journal, 4, 221-235.
- Mintzberg, H. (1978). Patterns in strategy formation. Management Science, 24(9), 934-948.
- Mintzberg, H. (1987). The strategy concept II: Another look at why organizations need strategies. California Management Review, 30(1), 25-32.
- Mintzberg, H., & McHugh, A. (1985) Strategy formation in an adhocracy. Administrative Science Quarterly, 30, 160-197.
- Mintzberg, H., & Waters, J. A. (1982). Tracking strategy in an entrepreneurial firm. Academy of Management Journal, 25(3), 465-499.
- Mintzberg, H., & Waters, J. A. (1985). Of strategies, deliberate and emergent. Strategic Management Journal, 6, 257-272.
- Mork, S. (1996). Protecting information assets. Bankers Magazine, 179, 23+. Retrieved December 1996, from Electric Library database (Infonautics Corporation) on the World Wide Web: <http://www.infonautics.com>
- Nadler, D. A., & Tushman, M. L. (1980). A congruence model for diagnosing organizational behavior. In R. Miles (Ed.), Resource book in macro organizational behavior. (pp. 30-49). Santa Clara, CA: Goodyear.
- National Research Council (1991). Computers at risk: Safe computing in the information age. Washington, DC: National Academy Press.
- Nelson, K. (1995). Combating viruses on microcomputers and LANs. Information Systems Security, 4, 55+. Retrieved August 1996, from Electric Library database (Infonautics Corporation) on the World Wide Web: <http://www.infonautics.com>

Nisbett, R. E., & Ross, L. (1980). Human inference: Strategies and shortcomings of social judgment. Englewood Cliffs, NJ: Prentice Hall.

Nonaka, I. (1991). The knowledge-creating company. Harvard Business Review, 69(6), 96-104.

Nunnally, J. C. (1978). Psychometric theory (2nd ed.). New York: McGraw-Hill.

Nunnally, J. C., & Bernstein, I. (1994). Psychometric theory (3rd ed.). New York: McGraw-Hill.

Ohmae, K. (1989). The global logic of strategic alliances. Harvard Business Review, 67(2), 143-154.

Oliver, R. L. (1980). A cognitive model of the antecedents and consequences of satisfaction decisions. Journal of Marketing Research, 17(4), 460-469.

Oliver, R. L., & DeSarbo, W. S. (1988). Response determinants in satisfaction judgements. Journal of Consumer Research, 14(4), 495-507.

O'Leary, J. (1995). Benchmarking your security program. Computer Security Journal 11(2), 25-34.

Olsen, D. A. (1995). A new realm of risk management. Risk Management, 42(7), 16-20.

Paddock, C. E., & Scamell, R. W. (1984). Office automation projects and their impact on organization, planning, and control. ACM Transactions on Office Information Systems, 2(4), 289-302.

Panettieri, J. C. (1994) Are your computers safe? Information Week, 28, November 1994, Retrieved March 2001, from the World Wide Web: <http://www.informationweek.com/507b/03mtsr.htm>

Panettieri, J. C. (1995) Information Week /Ernst & Young Security Survey: SECURITY. Information Week, 27, November 1995, Retrieved March 2001, from the World Wide Web: <http://www.informationweek.com/555/55mtsec.htm>

Papp, R., & Luftman, J. (1995). Business and I/T strategic alignment: New perspectives and assessments. Proceedings of AIS American Conference on Information Systems (pp. 1-6+), August 25-27, Pittsburg, PA. Retrieved October 1996, from <Http://hsb.baylor.edu/ramsower/acis/papers/papp.htm>

Parker, D. B. (1995). Possession as an element of information security. Information Systems Security, 4, 19+. Retrieved from Electric Library-Infonautics Corporation September 1996.

Parker, D. B. (1995b). From the editor. Information Systems Security, 4, 3+. Retrieved from Electric Library-Infonautics Corporation September 1996.

Parker, D. B. (1995c). Defining automated crime. Information Systems Security, 4, 16+. Retrieved from Electric Library-Infonautics Corporation September 1996.

Parker, D. B. (1996). Security as the target of criminals. Information Systems Security, 4, 14+. Retrieved from Electric Library-Infonautics Corporation September 1996.

Perschke, G. A. (1986). Micros in accounting: Four steps to information security. Journal of Accountancy, 176(4), 104-111.

Pettigrew, A. M. (1992). On studying managerial elites. Strategic Management Journal, 13, 163-182.

Plant, M. (1993). Getting management buy-in to IT security. Computers and Security, 12, 623-626.

Poore, R. (1995). Closed serve at the open net. Information Systems Security, 4, 22+. Retrieved from Electric Library-Infonautics Corporation September 1996.

Powell, P. (1992). Beyond networking: The rise of the nebulous organization, European Management Journal, 10(3), 352-356.

Porter, M. E. (1985). Competitive advantage: Creating and sustaining superior performance. New York: Free Press.

Porter, M. E., & Millar, V. E. (1985). How information gives you a competitive advantage. Harvard Business Review, 4, 149-160.

Prahalad, C. K., & Doz, Y. L. (1981). An approach to strategic controls in MNCs. Sloan Management Review, 22, 5-13.

Prahalad, C. K. & Hamel, G. (1990). The core competence of the corporation. Harvard Business Review, May-June, 79-91.

Price, R. L., Cotner, J. S., & Dickson, W. L. (1989). Computer fraud in commercial bank: Management's perception of risk. Journal of Systems Management, 40(10), 28-33.

Priem, R. L. (1990). Top management team group factors, Consensus and firm performance. Strategic Management Journal, 11, 469-478.

Priem, R. L., Rasheed, A. M. A., & Kotulic, A. G. (1995). Rationality in strategic decision processes, environmental dynamism and firm performance. Journal of Management, 21(5), 913-929.

Quinn, J. B. (1992). Intelligent enterprise: A knowledge and service based paradigm for industry. New York: Free Press.

Raho, L. E., & Belohlav, J. A. (1986). Strategic thinking and the personal computer/ Some policy consideration. Information Systems Management, 3(4), 52-57.

Raiffa (1968). Decision analysis. Reading, MA: Addison-Wesley.

Rainer, R. K., Snyder, C. A., & Carr, H. H. (1991). Risk analysis for information technology. Journal of Management Information Systems, 8(1), 129-147.

Rajagopalan, N., Rasheed, A. M. A., & Datta, D. K. (1992). Strategic decision processes: An integrative framework and future directions. In P. Lorange, B. Chakravarthy, J. Roos, & A. Van de Vans (Eds.), Strategic processes: Learning, adaptive and innovation. Basil, Switzerland: Blackwell.

Rangan, P. V. (1992). An axiomatic theory of trust in secure communication protocols. Computers and Security, 11(2), 163-172.

Regan, E. A., & O'Connor, B. N. (1994). End-user information systems: Perspectives for managers and information systems professionals. New York: Macmillan.

Reich, R. B. & Makin, R. (1986). Joint ventures with Japan give away our future. Harvard Business Review, 64, 78-86.

Reid, J. (1995). Open systems security: Traps and pitfalls. Computers and Security, 14, 496-517.

Risks-Forum Digest (1996b). Copy Editor, 18(10).

Risks-Forum Digest (1996a). Copy Editor, 18(4).

Robey, D., & Sahay, S. (1996). Transforming work through information technology. Information Systems Research, 7(1), 93-110.

Rockart, J. F., Earl, M.J., & Ross, J. W. (1996). IT in the 1990s: Managing organizational interdependence. Sloan Management Review, 30(2), 7-17

Rockart, J. F., & Short, J. E. (1991). The networked organization and the management of interdependence. In E. Michael & S. Scott Morton (Eds.), The corporation of the 1990s: Information technology and organizational transformation (pp. 189-219). New York: Oxford University Press.

Ross, S. A. (1981). Some stronger measures of risk aversion in the small and in the large with applications. Econometrica, 49, 621-638.

- Rumelt, R. P. (1974). Strategy, structure, and economic performance. Cambridge, MA: Harvard University Press.
- Sambamurthy, V., Zmud, R. W., & Boynton, A. C. (1994). The determinants of business unit reliance on information technologies. In N. Venkatraman & J. Henderson (Eds.), Research in strategic management and information technology (Vol. 1). Greenwich, CT: JAI Press.
- Schendel, D. E., & Patton, R. G. (1978). A simultaneous equation model of corporate strategy. Management Science, 24, 1611-1621.
- Schwab, D. P. (1980). Construct validity in organizational behavior. In B. M. Straw & L. L. Cummings (Eds.), Research in organizational behavior (Vol. 2) (pp. 3-43). Greenwich, CT: JAI Press.
- Scott Morton, M. (Ed.). (1991). The corporation of the 1990s. Oxford: Oxford University Press.
- Seddon, P. B. (1997). A respecification and extension of the DeLone and McLean Model of IS success. Information Systems Research, 8(3), 240-253.
- Sethi, V., & King, W. R. (1991). Construct measurement in information systems research: An illustration in strategic systems. Decision Sciences Journal, 22(3), 455-472.
- Settembrind, F. (1994). Risk management in enterprise: A systematic approach. Risk Management, 41(8), 34-37.
- Shannon, C., & Weaver, W. (1949). The mathematical theory of communications. Urbana, IL: University of Illinois Press.
- Sherer, S. A. (1995). Risk in interorganizational information systems. Proceedings of AIS American Conference on Information Systems, August 25-27, Pittsburg, PA, pp. 1-5+. Retrieved 1996, from [Http://hsb.baylor.edu/ramsower/acis/papers/sherer.htm](http://hsb.baylor.edu/ramsower/acis/papers/sherer.htm)

Shirani, A., Aiken, M., & Reithel, B. (1994). A model of user information satisfaction. Data Base, 25(4), 17-23.

Shortell, S. M. & Zajac, E. J. (1990). Perceptual and archival measures of miles and snow's strategic types: A comprehensive assessment of reliability and validity. Academy of Management Journal, 33(4), 817-832.

Shrivastava, P., & Grant, J. H. (1985). Empirically derived models of strategic decision-making processes. Strategic Management Journal, 6(2), 97-113.

Shtub, A., Bard, J. F., & Globerson, S. (1994). Project management: engineering, technology and implementation. London: Prentice Hall.

Sitkin, S. B., & Weingart, L. R. (1995). Determinants of risky decision-making behavior: A test of the mediating role of risk perceptions and propensity. Academy of Management Journal, 38(6), 1573-1592.

Slovic, P. (1964). Assessment of risk taking behavior. Psychological Bulletin, 61(3), 220-233.

Slovic, P. (1987). Perception of risk. Science, 236, 280-286.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1977). Behavioral decision theory. In M. R. Rosenzweig & L. W. Porter (Eds.), Annual review of psychology (pp. 1-39). Palo Alto, CA: Annual Reviews.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1977a). Preference for insuring against probable small losses. Journal of Risk and Insurance, 44(2) 237-258.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1982). Fact versus fears: Understanding perceived risk. In D. Kahneman, P. Slovic & A. Tversky (Eds.), Judgment under uncertainty: Heuristics and biases (pp. 463-489). New York: Cambridge University Press.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1986). The psychometric study of risk perception. In V. T. Coello, J. Menkes, & J. Mumpower (Eds.), Risk evaluation and management. New York: Plenum.

Smircich, L., & Stubbart, C. (1985). Strategic management in an enacted world. Academy of Management Review, 10(4), 724-736.

Smith, J. (1995). How to investigate and prosecute network intrusions. Computer Security Journal, 11(2), 47-54.

Sommer, P. (1994). Industrial espionage: Analyzing the risk. Computers and Security, 13(7), 558-563.

Sparks, P., & Shepherd, R. (1994). Public perceptions of the potential hazards associated with food production and food consumption: An empirical study. Risk Analysis, 14(5), 799-806.

Spender, J. C. (1989). Industry recipes: An enquiry into the nature and sources of managerial judgement. Oxford: Basil Blackwell.

Stahl, S. H. (1993). Information security in workstation environments. Computers and Security, 12(2), 117-122.

Stephanou, H. E. (1987). Perspectives on imperfect information processing. IEEE Transactions on Systems, Man, and Cybernetics, 17(5).

Sterne, D. F. (1991). On the buzzword "security policy." Proceedings, 1991 IEEE Computer Society symposium on research in security and privacy (pp. 219-230), May 20-22, Oakland, CA. Los Alamitos, CA: IEEE Computer Society Press.

Stewart, T. A. (1992). The search for the organization of tomorrow. Fortune, 125(10), 92-98.

Straub, D. W. (1989). Validating instruments in MIS research. MIS Quarterly, 13(2), 147-169.

- Straub, D. W. (1990). Effective IS security: An empirical study. Information Systems Research, 1(3), 255-276.
- Strauss, A., & Corbin, J. (1990). Basics of qualitative research. Newbury Park, CA: Sage.
- Subramamian, A., & Nilakanta, S. (1994). Measurement: A blueprint for theory-building in MIS. Information and Management, 26, 13-20.
- Suh, K., Kim, S. & Lee, J. (1994). End-user's disconfirmed expectations and the success of information systems. Information Resources Management Journal, 7(4), 30-39.
- Szajna, B. (1993). Determining information system usage: Some issues and examples. Information and Management, 25, 147-154.
- Tabachnick, B. G., & Fidell, L. S. (1989). Using multivariate statistics (2nd ed.). New York: Harper & Row.
- Tan, D. (1995). IT management plateaus: An organizational architecture for IS. Information Systems Management, 12, 44+. Retrieved from Electric Library-Infonautics Corporation April 1996.
- Tapscott, D., & Caston, A. (1993). Paradigm shift: The new promise of information technology. New York: McGraw-Hill.
- Thompson, B. (1995). First-aid for the computer disaster. Corporate Report-Minnesota. 26, 27+. Retrieved June 1996, from Electric Library database Infonautics Corporation on the World Wide Web: <http://www.infonautics.com>.
- Thompson, J. D. (1967). Organizations in action: Social science bases of administrative theory. New York: McGraw-Hill.
- Thong, J. Y. L., Yap, C., & Raman, K. S. (1996). Top management support, external expertise and information systems implementation in small businesses. Information Systems Research, 7(2), 248-267).

Tipton, H. (1994). Liability of corporate officers for security problems. Computer Security Journal, 10(1), 59-69.

Tomaskovic-Devey, D., Leiter, J., & Thompson, S. (1994). Organizational survey nonresponse. Administrative Science Quarterly, 39, 439+. Retrieved August 1996, from Electric Library database Infonautics Corporation on the World Wide Web: <http://www.infonautics.com>.

Troy, E. G. (1995). A rebirth of risk management. Risk Management, 42(7), 71-73.

Tse, D. K., Nicosia, F. M., & Wilton, P. C. (1990). Consumer satisfaction as a process. Psychology and Marketing, 7(3), 177-193.

Tse, D. K., & Wilton, P. C. (1988). Models of consumer satisfaction formation: An extension. Journal of Marketing Research, 204-212.

Tully, S. (1993). The modular corporation. Fortune, 127(3), 106-115.

Tushman, M. L., & Nadler, D. A. (1978). Information processing as an integrating concept in organizational design. Academy of Management Review, 3(3), 613-624.

Venkatraman, N. (1989). The concept of fit in strategy research: Toward verbal and statistical correspondence. Academy of Management Review, 14(3), 432-444.

Venkatraman, N.; (1989a). Strategic orientation of business enterprises: The construct, dimensionality, and measurement. Management Science, 15(8), 942-961.

Venkatraman, N. (1994). IT-enabled business transformation: From automation to business scope redefinition. Sloan Management Review, Winter, 73-87.

Venkatraman, N., & Grant, J. H. (1986). Construct measurement in organizational strategy research: A critique and proposal. Academy of Management Review, 11(1), 71-87.

Venkatraman, N., & Prescott, J. E. (1990). Environment-strategy coalignment: An empirical test of its performance implications. Strategic Management Journal, 11(1), 1-24.

Violino, B. (1996). Word macro viruses to cost companies billions of dollars: E-mail spreads the threat. Information Week, 1, April 1996, pp. 22+. Retrieved March 2001, from the World Wide Web: <http://www.informationweek.com/573/73iuvir.htm>

Violino, B. (1996b). The security façade: Are organizations doing enough to protect themselves? This year's IW/Ernst & Young survey will shock you. Information Week, 21 October, 1996. Retrieved March 2001, from the World Wide Web: <http://www.informationweek.com/602/02mtsec.htm>

Violino, B. (1996c). Intranets: Not safe, either. Information Week, 19, February, 1996 Retrieved March 1996, from the World Wide Web: <http://www.informationweek.com/>

Vitale, M. R. (1986). The growing risks of information systems success. MIS Quarterly, 10(4) 327-334).

Vojta, G. J. (1992). Build a framework for risk management. Financial Executive, 8(6), 34-37.

von Solms, R., Eloff, J. H. P., & von Solms, S. H. (1990). Computer security management: A framework for effective management involvement. Information Age, 12(4), 217-222.

von Solms, R., van de Haar, H., von Solms, S. H., & Caelli, W. J. (1994). A framework for information security evaluation. Information and Management, 26(3), 143-153.

Wallsten, T. S. (1980). Cognitive processes in choice and decision behavior. New Jersey: Lawrence Erlbaum.

Wang, P., & Chan, P. S. (1995). Top management perception of strategic information processing in a turbulent environment. Leadership and Organizational Development Journal, 16(7), 33-43.

♦

- Warman, A. R. (1993). Computer security within organizations. London: Macmillan.
- Webster's New Collegiate Dictionary. (1957). Thin paper. Springfield, MA: C. Merriam.
- Weick, K. (1979). The social psychology of organizing (2nd ed.). Readings, MA: Addison-Wesley.
- Wessler, J., Myers, E., & Gardner, W. D. (1971). Physical security: facts and fancies. Datamation, 17(13), 34-37.
- Wharton, F. (1992). Risk management: Basic concepts and general principles. In J. Ansell & F. Wharton (Eds), Risk: Analysis, assessment and management. London: John Wiley.
- White, D. E., & Farrell, M. H. (1994). Reengineering information security administration. Computer Security Journal, 10(1), 23-37.
- White, M. (1991). Who will win in the outsourcing stakes? Communications International, December, 19-20.
- Willcocks, L. (1992). Evaluating information technology investments: Research findings and reappraisal. Journal of Information Systems, 2(3), 1-26.
- Willcocks, L., & Margetts, H. (1994). Risk assessment and information systems. European Journal of Information Systems: An Official Journal of the Operations Research Society, 3(2), 27-138.
- Wood, C. C. (1991). Using information security to achieve competitive advantage. Computers and Security, 10, 399-404.
- Wood, C. C. (1994). Using network management systems to achieve information security. Computer Security Journal, 10(1), 11-21.
- Wood, C. C. (1995). Shifting information systems security responsibility from user organizations to endor/publisher organizations. Computers and Security, 14, 283-284.

Wood, C. C. (1995b). Writing InfoSec policies. Computers and Security, 14, 667-674.

Woodward, J. (1965). Industrial organization: Theory and practice. London: Oxford University Press.

Work, C. P. (1988, June 20). Business without borders. U.S. News & World Report, pp. 48-53.

Yap, C. S., Soh, C. P. P., & Raman, K. S. (1992). International systems success factors for business. OMEGA International Journal of Management Sciences, 5(6), 597-609.

Yin, R. K. (1989). Case study research: Design and methods (Vol 5). Newbury Park, CA: Sage.

Zajac, E. J., & Shortell, S. M. (1989) Changing generic strategies: Likelihood, direction, and performance implications. Strategic Management Journal, 10, 413-430.

Zona Research. (1999). Infrastructure and management: Focus of business critical internet security. White Paper downloaded from Zona Research Inc. web site. <http://www.zonaresearch.com/deliverables/white%5Fpapers/wp19/index.htm>.

BIOGRAPHICAL STATEMENT

Andrew G. Kotulic received his Ph.D. in Business Administration from The University of Texas at Arlington in May 2001. He earned a Master of Business Administration from the Illinois Institute of Technology in 1973 and a Bachelor of Science in Industrial Engineering from the Illinois Institute of Technology in 1966.

Dr. Kotulic has held academic positions as an Assistant Professor of Information Systems at York College of Pennsylvania; Visiting Assistant Professor of Computer Information Systems at the University of Louisiana at Monroe; a Lecturer in Management at Al Akhawayn University in Ifrane, Morocco; and as a Graduate Teaching Associate at The University of Texas at Arlington.

His academic honors include receiving the John Deane Stanley Foundation Scholarship for 1991–92, awarded to a Ph.D. student major/minor in strategic management at The University of Texas at Arlington; a member of Sigma Iota Epsilon-Honorary Management Fraternity; a member of Alpha Pi Mu-Industrial Engineering Honor Society. Additionally, Dr. Kotulic coauthored "Rationality in Strategic Decision Processes, Environmental Dynamism and Firm Performance" with R. L. Priem and A. Rasheed. The paper won the 1996 Distinguished Professional Publication Award Honorable Mention, College of Business Administration, The University of Texas at Arlington.

Dr. Kotulic has held positions in industry at Northrop Corporation Defense Systems Division; Sara Lee Corporation; MCC/Powers Corporation; Milton Bradley Corporation-Playskool Division and Motorola Inc-Communications Division.

