Critical Success Factors for an Effective Security Risk Management Program: An Exploratory Case Study

Abstract

This paper evaluates the perceived effectiveness of the security risk management (SRM) programs at two Fortune 500 firms using qualitative (interviews) and quantitative (survey) methods. Layers of management (executive, middle, and lower), and staff from both firms participated in the study. Perceived effectiveness of their SRM programs was based on nine critical success factors (CSFs). Six initial critical success factors (CSFs): Executive Management Support, Organizational Maturity, Open Communication, Risk Management Stakeholders, Team Member Empowerment, and Holistic View of an Organization were extracted from organizational role theory. They were confirmed and synthesized with three additional CSFs (Security Maintenance, Corporate Security Strategy, and Human Resource Development). A survey based on the CSFs was implemented at the two firms. Although both firms are Fortune 500 technology companies, their perceptions of current perceived SRM effectiveness differ significantly.

Keywords: Information security, security risk management, critical success factors

Critical Success Factors for an Effective Security Risk Management Program: An Exploratory Case Study

INTRODUCTION

The most recent Ernst & Young Global Information Security Survey (Bandyopadhyay et al. 2009) shows that organizations are increasingly recognizing information security risks and are improving the effectiveness of their information security programs. However, a large portion (64%) of the survey respondents indicated that the level of employee security awareness was either a significant or a considerable challenge in meeting their information security initiatives. Lack of compliance with information security policies is a major problem (Siponen and Vance 2010). In addition, outsider threats, such as viruses and system penetration attacks continue to increase in cost and complexity.

Traditionally, IS security research has focused on its technological aspects. However, the problem has a "behavioral root" (Workman and Gathegi 2007) and is subject to both psychological and sociological actions of people (Parker 1981). Recent research has focused on insider threats (Sneha and Varshney 2009). Since users interact with information systems on a regular basis in their business activities, how they use the systems and whether they follow established measures will ultimately influence the overall security of an organization's information systems.

Information security is a phenomenon that occurs in waves, progressing from technical to managerial to institutional and finally to information security governance (von Solms et al. 1994). Although methods of research in information security have been proposed and compared at length (Siponen 2005), there exist few organizational level studies that employ theoretical rigor. Organizational systems are less secure if top managers, middle managers, and employees

neglect information security procedures (Straub and Welke 1998). Studies have shown that issues become more complex when executive management is unable to view risk from all perspectives (March and Shapira 1987). For example, management may not consider risk takers motivated by factors other than personal incentives. They may also believe that organizations generally inhibit risk taking.

Security risk management (SRM) refers to a series of mechanisms put in place by an organization to counter or prevent information security related events (Blakley et al. 2001). Examples of such mechanisms include implementation of clearly defined information security policies and secure computing practices (Spears and Barki 2010). An information security event may include factors such as insider threat, malware, and unauthorized access. Since SRM impacts the organization as a whole and focuses on confidentiality, integrity, and availability of data, it is imperative that effective SRM policies and practices be established and followed.

The overall objective of SRM is to enable an organization to handle information and data adequately. As such, data and information should be safe from potential threats. SRM is not a standalone activity. Instead it should be an integral part of the processes throughout an organization (Dhillon 2007). This includes addressing potential threats, educating personnel in security awareness, and establishing and executing security policies. Considering the overarching impact of an SRM program, it is surprising to note that little research has been conducted in this area.

Kotulic (2001) developed an instrument that provided a starting point for the development of theory-based guidelines to manage the SRM process. His model included a direct relation between executive management support and SRM program effectiveness.

However, he was unable to test his theoretical model. Although he had confirmed focused interviews with five firms, all firms declined when they saw the preliminary questionnaire. Over a course of several months, he contacted 38 additional firms. Finally, one firm agreed to participate in the study, but on a limited basis. Based on interview results, the survey questionnaire was modified and sent to over 1,500 top management team members of large (greater than 500 employees) firms. Unfortunately, less than 100 surveys were returned, resulting in a response rate of less than 2%. This was attributed to the sensitive nature and complexity of the survey questions (Kotulic and Clark 2004).

In order to be effective, security controls must be in line with the goals and objectives of an organization (Gatzlaff and McCullough 2010; Khansa and Liginlal 2011; Spears and Barki 2010; Zhuang 2005). Therefore, it is important to focus on the information needed to attain these goals and objectives. Critical success factors (CSF) are "things" that must go well to ensure success for a manager or an organization (Rockart 1979). We purport that employee (management or staff) understanding of CSFs as they relate to SRM can allow an organization to maximize the overall effectiveness of its SRM program. Therefore, we expanded upon Kotulic's research by incorporating a modified version of the CSF method. Initial CSFs were extracted from Role Theory, which provides insight into recurring patterns of actions that are considered important for effective role functioning in an organization (Kahn et al. 1964). We believe this was necessary to not only provide theoretical rigor, but also assist in easing some of the concerns the organizations may have had about an intrusive topic such as information security. Through a series of interviews, we extracted additional CSFs, which formed the basis of a synthesized list of CSFs.

The purpose of this study was twofold: 1) identify CSFs as they relate to SRM, as perceived by both management and staff, and 2) ascertain how management and staff perceive the effectiveness of their SRM policies and procedures in attaining the goals associated with these CSFs. Currently, no known studies have concentrated on the link between management and staff in terms of establishing and maintaining effective SRM policies. Executive management may have varying perspectives of expected SRM strategies than those of the staff. This can impact the actual effectiveness of SRM strategies. Therefore, the primary research question addressed in this study is: What is the CSF impact on the perceived effectiveness of an organization's SRM program?

The remainder of this paper is organized as follows. First, we provide a literature review, focusing on CSFs and SRM. Next, we describe our mixed method research design, along with detailed discussion of both qualitative and quantitative portions of the study. This is followed by detailed discussion of the results and contributions to practice. We conclude the paper by discussing limitations and suggestions for future research.

LITERATURE REVIEW

This section first focuses on studies that investigated the critical success factors concept, followed by studies pertaining to organizational information security.

Critical Success Factors (CSF)

The CSF method was initially proposed (Rockart 1979) to help CEOs specify their information needs related to critical firm issues so that systems could be developed to meet those needs. CSFs are intended performance consequences of systems and behaviors within the firm, which are strongly related to the achievement of desired firm objectives. Benefits of CSFs

include 1) identifying factors for management scrutiny developing, 2) establishing measures for evaluation, 3) focusing attention on significant data to be collected, 4) accommodating change within an organization, and 5) assisting in the planning process (Rockart 1979).

In IS, the CSF method has been introduced as a mechanism for aligning IT planning with the strategic direction of an organization (Rockart 1979). User acceptance is a major benefit of using the CSF method. Managers seem to intuitively understand the thrust of the CSF method and endorse its usage as a means of identifying areas of concern in an organization (Boynton and Zmud 1984). CSFs can also be used as an MIS planning tool by interviewing multiple levels of managers in an organization (Bullen and Rockart 1981). Other CSF research in the IS discipline includes areas such as the IS development process (Butler and Fitzgerald 1999), IS planning (Bowman et al. 1983), organizational performance (Ponemon 2010), performance evaluation (Bergeron and Begin 1989), e-commerce (Riddell 2011), ERP systems (Bayus et al. 2003), data management (Guynes and Vanecek 1996), e-banking (Dehning et al. 2007), and inter-organizational information system (Mukherjee 2008). In the areas of security risk management, organizational factors including IT competence of business managers, environment uncertainty, industry type, and organization size were found to impact the effectiveness of implementing information systems (Tsoumas and Gritzalis 2006).

Organizational level studies that consider SRM in the context of an actual business setting are currently lacking in IS research (Weiser 1991). This might be due to the fact that security is considered to be intrusive in nature (Kotulic and Clark 2004). The following section provides a review of information systems security policies proposed and their use in the organizations.

Effectiveness of Deterrence Measures

Most prior research in organizational IS security has dealt with success and failure of security policies. General Deterrence Theory (GDT) has been used to investigate the effect of organizational deterrent measures on computer abuses by employees. Deterrent measures can reduce computer abuse by potential offenders if the risk of punishment is high (deterrent certainty) and penalties for violations are severe (deterrent severity) (Straub 1990). However, findings regarding the effectiveness of deterrence measures are mixed. Deterrent and preventive methods have a positive impact on information security effectiveness (Straub 1990), but severity of the deterrence method does not (Kankanhalli et al. 2003). But contrary to what is proposed by GDT, organizations with a high number of deterrent measures have higher incidents of insider abuse (Lee et al. 2004), indicating a significant negative relation between deterrent measures and insider abuse.

An extended GDT model (D'Arcy et al. 2009) showed no relation between perceived certainty of sanctions and intention of misuse. However, security policy awareness reduced perceived certainty of sanction. While this negative relation may have been due to factors such as research design and user knowledge about the difficulties in detecting misuse incidents (D'Arcy et al. 2009), it may also be that user attitude toward the policies influenced the relation. A user may be under the impression that policies exist only on paper and not enforced, even though the punishments of violation may be severe; therefore, employee actions may reflect that belief.

Security Policies Compliance

Prior studies have focused on employee compliance to security policies. An Information Security Policy Compliance Model suggests that a user's intention to comply with security

policies is influenced by user attitude toward complying (Pahnila et al. 2007). User's attitude and intention are influenced by a mixture of negative and positive reinforcements. Examples of negative reinforcements include sanctions, threat appraisal, coping appraisal, and normative beliefs. Positive reinforcements include information quality of policies, facilitation conditions, and habits. In a similar study, the antecedents of employee compliance with information security policy (ISP) of an organization were investigated (Sneha and Varshney 2009). The study indicated that an employee's attitude positively influences an employee's intention to comply with the ISP. In addition, information security awareness significantly influenced an employee's attitude to comply with the ISP through the employee's beliefs.

A compliance model for employees in an organization suggested that user compliant behavioral intention is influenced by the information security environment perceived by the users and their self-efficacy (of breaching security) (Chan et al. 2005). User perception of the security environment is determined by an employee's observation of top management practices, direct supervisory practices, and socialization among coworkers. Another study focused on why employees fail to implement information security threats and countermeasures even though they are aware of them (Workman et al. 2008). The study indicated that the extent to which people perceive the severity of a threat dictates how motivated they are to prevent it from happening.

Using a neutralization model to study the problem of employee information security violations, researchers found that employees rationalized their violations of security policies (Siponen and Vance 2010). Neutralization had a significant impact on an employee's intention to violate information systems security policies. However, formal and information sanctions had no significant effect. Using a mixed research design to examine user participation in IS SRM, researchers found that user participation is an important factor for improving security control

performance (Spears and Barki 2010). User participation raised organizational awareness of security risks and controls, facilitated alignment of SRM with business objectives, and improved environmental control.

The next section explains the research method used in this study.

RESEARCH METHOD

We modified the CSF method by incorporating the use of role theory to extract a set of initial CSFs. This is detailed next.

Initial CSFs Based on Role Theory

As shown, prior research in organizational information security has mostly been associated with deterrence measures using certain security policies. Since management and staff may have various beliefs regarding the effectiveness of an organization's SRM policies, exploring these differences in perception increases our understanding of SRM effectiveness.

The CSF method has traditionally followed an interpretivist paradigm in prior research. We extended the CSF method to include quantitative research methods supported by a positivist paradigm.

Role theory, developed in the 1960s, provides insight into the recurring patterns of actions that are considered important for effective functioning in a particular role (Kahn et al. 1964). It focuses on individual roles within an organization and the interaction between roles and the impact on achieving organizational goals (Katz and Kahn 1978). Since employee (management or staff) actions are directly related to work performance, understanding determinants of employee actions is a major step toward an effective SRM. Therefore, we

extracted initial CSFs from the Role Theory literature, which has five primary tenets. They are Role Conflict, Role Ambiguity, Role Compliance, Communication, and Role Consensus. While each tenet has appeared in various IS studies, it has not appeared in its entirety in IS literature. In the following section, we provide a description of each tenet followed by the extracted CSF (or CSFs) from the tenet.

Role Conflict

Prior Role Theory research has shown that Role Conflict leads to decreased organizational performance and effectiveness (Baroudi 1985). Role Conflict can arise when different members of an organization may hold different expectations for a focal person's role or when a set of role demands by management contains internally contradictory expectations (McGrath 1976). In order to avoid issues related to Role Conflict, a major portion of the stakeholders should be considered. In the case of SRM, stakeholders include all management and staff since all workers in an organization need to understand and adhere to its policies and procedures in order to protect their assets. Thus, we considered *Risk Management Stakeholders* as a surrogate CSF for Role Conflict. In this study, *Risk Management Stakeholders* include a broad base of workers to elaborate what is important to an organization while generating new ideas (Peffers et al. 2003).

Role Ambiguity

Role Ambiguity relates to uncertainty about what an employee in an organization is allowed to do (Biddle and Thomas 1966; Katz and Kahn 1978). There is evidence that Role Ambiguity impacts task effectiveness in an organization. Prior studies have shown that lack of employee empowerment reduces the effectiveness of tasks (Cohen 1959; Smith 1957). In

another study, researchers concluded that executive management's uncertainty due to lack of sufficient information impacted organizational performance (Shenkar and Zeira 1992). Role Ambiguity can be reduced if workers in an organization have a certain degree of empowerment with regard to decision making (Conger and Kanungo 1988). Thus, employee empowerment leads toward a more effective implementation of management policy decisions. Organizational success, which embodies significant empowerment through self-management teams, has been explored extensively in previous research and is widely regarded as a CSF (Al-Mashari and Zairi 1999). Thus, we consider *Team Member Empowerment* as a surrogate CSF for Role Ambiguity. In this study, we define *Team Member Empowerment* as the resources available to employees for making decisions regarding the SRM program.

Role Compliance

In regard to Role Compliance, each employee has a set of allowable behaviors and actions that are well defined as part of an organization policy. Whenever a situation of non-compliance arises, an organization can use its existing policy structure to employ different types of sanctions (Katz and Kahn 1978). Compliance is a necessary step toward achieving maturity in an organization's security policies (Paulk et al. 1993). In mature organizations, systems are formalized and produce data appropriate to their decision and control processes (Ein-Dor and Segev 1978). Following other researchers' views that organizational maturity is a CSF for successful implementation of IT solutions (Magal et al. 1988; Martin 1982), we consider *Organizational Maturity* a surrogate CSF for Role Compliance. In this study, we define *Organizational Maturity* as a set of initial formal or informal procedures that are in place to counter issues related to information security.

Communication

Communication is a social process of the broadest relevance in the functioning of an organization. The full and free flow of information across all organizational levels is a healthy step forward in avoiding intra-organizational problems (Katz and Kahn 1978). IS literature has emphasized the usefulness of effective communication (Delone and McLean 2003). The free flow of information not only reduces the risk of misunderstanding but also ensures that all stakeholders can contribute as a team. Especially during times of crisis, inter- and cross-departmental communication is a CSF (Akkermans and van Helden 2002). Thus, we consider O*pen Communication* a surrogate CSF for Communication. In this study, we define *Open Communication* as the free flow of information among the SRM team and the risk management stakeholders.

Effective communication is best achieved if a project leader has a clear and holistic view of an organization (Kidd et al. 1999). Invariably, what is beneficial for a single department may not be beneficial for the organization as a whole. An holistic approach to decision making therefore serves as a CSF for organization wide projects (Lam 2005). Thus, we consider *Holistic view of an Organization* a surrogate CSF for Communication.

Role Consensus

Role Consensus is the degree to which management believes in a policy by working closely with employees (Katz and Kahn 1978). There is widespread agreement of the need for participative decision making in regard to implementing a policy (Tannenbaum and Cooke 1978). Top management support is the most important factor in preventing project failures (Schmidt et al. 2001). Management should be actively concerned with planning, standardization of policies and procedures along with its employees. If SRM is supported from the top, the

organization is better able to articulate security in terms of business value. Management support has previously been classified as a CSF (Martin 1982). Thus, we consider *Executive Management Support* a surrogate CSF for Role Consensus. In this study, we define *Executive Management Support* as enthusiastic support in the form of personnel or financial resources, or participation in the review of findings and recommendations of the SRM process.

Accordingly, we extracted six initial CSFs derived from the existing Role Theory literature. They are *Executive Management Support, Organizational Maturity, Open Communication, Risk Management Stakeholders, Team Member Empowerment, and Holistic View of an Organization.* These initial CSFs were a starting point for our study.

Mixed Method Research Design

We employed a mixed method research design approach that incorporated a combination of data collection and analysis methods on separate samples to examine user perception of SRM effectiveness. Data were collected at two firms, Companies A and B. Both are multinational Fortune 500 technology firms with established security risk management programs. We concentrated on a single location for each firm. Each location was within the United States, but in different parts of the country. Participants belonged to different layers of management (i.e., executive management, middle management, and lower management) and staff. We only considered full-time employees. In both companies, there were a greater number of staff participants, compared with management. However, this is not considered a limitation of the study, since an effective organization will typically have a pyramid structure (Sennewald 2003). Qualitative (using interviews) and quantitative data (using a survey) were collected at Company A. Management and staff at Company B responded to the same survey that was used for Company A.

Various researchers have addressed methodological issues such as lack of control and generalizability that arise when a case study is conducted (Datta 1982; Dukes 1965; Huberman and Crandall 1982; Miles 1982). To counter these issues, guidelines have been presented for the positivist case research paradigm (Lee 1989; Yin 1994). These guidelines have also been successfully applied (Sarker and Lee 2003) and are summarized in Table 1. This section explains techniques that have been shown to enhance research rigor and how they were implemented in this study. We also enhanced the guidelines, as indicated in the table.

Table 1: Research Rigor[1] of the Study Adapted from Lee (1989) and Yin (1994)

Criterion	**Guidelines**	**How the Guidelines Were Followed in this Study**
Internal validity	Pattern matching	"Natural Controls" were used whenever possible. *Interviews completed within approximately one month to prevent maturation effect.*
Construct validity	Using multiple sources Key informants will review the report	Multiple interviews with multiple stakeholders were carried out via interaction modes such as email, telephone, et cetera. Members of the executive team were provided with a draft of the case study. *A priori list of CSFs from theory*
External Validity	Increasing degrees of freedom	Multiple observations for each prediction. *Random selection of participants*
Statistical Conclusion Validity	*Sample Size*	*Homogeneity of participants*
Reliability	Creation of a case study resource list Case study protocol	Case study notes, documents (questionnaires, summary tables), and narratives. An evolving set of questionnaires, and literature review.
Data Triangulation	*Converging lines of inquiry*	*Use of interviews, observation, and questionnaires.*

[1] Italicized text indicates additions made to Lee (1989) and Yin's (1994) recommendations as part of providing research rigor to this study.

Since information security is considered a naturally intrusive topic, extensive informal conversations between the researcher and some of the management at both companies (Company A and Company B) had already taken place prior to execution of the study. The CSF method was selected due to its nature of relying on dialogue, hence easing management concerns about the topic. This allowed the development of a reasonably comfortable relationship between employees of both companies and the researcher, which is an essential component of security based research (Kotulic and Clark 2004). Prior communication also allowed Company A to grant us permission to study the in-depth aspects of their SRM implementation through interviews and questionnaires, which formed the core component of a CSF-based case study. On the other hand, Company B's employees were asked to complete the same survey that was administered at Company A. This allowed us to compare quantitative results at both companies.

Qualitative Data Collection at Company A via CSF Method

There is no standard procedure for CSF data collection and analysis (Bergeron and Begin 1989). Rockart (1979) suggested that CSFs should be collected during three to six hours of interviews with the CEO, but his concept only focused on the CEO's information requirements. As the problem and organizational scope of CSFs has broadened, consultants and researchers have used alternative methods such as "onion technique" interviews and analysis of interrelated organizational activities (Dickinson et al. 1985), an *a priori* list of CSFs from literature and a mailed questionnaire (Sabherwal and Kirs 1994), and most importantly interviews followed by questionnaires to implement CSFs (Guynes and Vanecek 1996).

To confirm/disconfirm the initial CSFs, structured and unstructured interviews were conducted with key personnel across all layers of management and staff. In all, 32 employees at Company A took part in this portion of the study. These employees were randomly selected, and

notified in advance about the option of interviewing. The breakdown of employees by level of employment is presented in Table 2.

Table 2: Interviewed Employees

Employee Level	Total	# Scenarios
Executive Management	2	2
Middle Management	3	2
Lower Management	9	2
Staff	18	8
Total	32	14

As part of the CSF confirmation/disconfirmation process, each participant was asked to create hypothetical scenarios (vignettes) related to potential violations of an SRM policy and their impact on Company A. Unlike the standard use of researcher-provided scenarios (Wason et al. 2002), we asked the participants to create their own scenarios, based on situations that were mentioned in Company A's SRM policy. The use of vignettes is recommended as a way of relating to sensitive survey questions (Lee 1993). We contend that presenting a respondent with an opportunity to create a scenario rather than asking direct questions about their organization's SRM policies resulted in a more honest gauge of their perceptions regarding information security.

As shown in Table 2, 14 of the 32 interviewees provided scenarios. Examples of the scenarios are presented in Appendix B. From these scenarios, we were able to glean quite a few points. Management scenarios were more concrete and highlighted a more strategic level of thinking and greater understanding of the SRM process. For example, an executive manager's scenario (see Appendix B Scenario 1) clearly specified the process in the event an employee deleted a customer's file. Conversely, staff scenarios (for example, refer to Appendix B

Scenario 2) had a much narrower scope, focusing more on an immediate advantage in a position of authority as opposed to the consequences of an action.

Confirmation of Initial CSFs and Extraction of New CSFs

As each interview progressed there was clearly a difference in opinion between management and staff with regard to the most important components of an effective SRM program. Senior members of the SRM management team were acutely aware of the challenges Company A faced in developing an SRM program that complied with both U.S. and European regulations. Since it is a global organization, this was one of the critical requirements for Company A. According to one executive, Company A dealt with a patchwork of "disparate and over-lapping state and federal regulations, along with privacy rules laid out by individual corporate partners." Within the European Union, it dealt with "the data protection directive, which unlike U.S. regulations such as HIPAA or Sarbanes-Oxley acts, provides few specifics as to how these privacy requirements should be met." While creating the SRM program, management therefore focused on the need to establish a consistent set of requirements common to various U.S. and EU jurisdictions, while keeping in mind Company A's own standards for protecting customer and supplier data. This was through enhanced security features such as encryption. This was also why, according to a middle manager, Company A focused on creating in-house security tools as part of their corporate security strategy. It allowed the organization to build a foundation that was both deep and broad, rather than a series of narrow solutions that addressed regulations on a case-by-case basis.

Overall, staff knew very little about the various U.S. and EU directives. However, most members of staff agreed that it was important to encourage growth of corporate security strategies because it made the organization proactive instead of reactive. This, according to a

staff member, also “prevented waste of staffing and budget resources.” The same person elaborated on how the current method of assessing the SRM program also had its disadvantages. Accordingly, when a division was informed that an assessment would occur, it changed its current practices to what was required as part of the SRM program. However, as soon as the division passed the assessment, the makeshift (required) processes were removed in favor of the initial practices.

Although most staff members were not familiar with the plethora of multi-national compliance requirements Company A was required to follow, they were well versed in other security services such as access control, encryption, employee training, and policy updates. According to a staff employee, Company A "is not immune to threats such as cyber-theft, and cyber-espionage by hackers, malware, and malicious insiders. It now uses logs for forensic analysis, and has detailed access control procedures, to try to prevent all types of cyber security incidents.” Both management and staff concurred on the importance of updating policies. According to management, business divisions usually initiated risk assessments based on each division’s prior results. Division heads were primarily responsible for ensuring that recommendations were implemented and that periodic updates were conducted and verified.

Discussions during these interviews confirmed the significance of the 6 initial CSFs and resulted in three additional CSFs: *security maintenance*, *corporate security strategy*, and *human resource development*. In subsequent interviews, the personnel were presented a final list of CSFs, and these CSFs were agreed upon by both management and staff. A point to note is that we obtained no new information regarding CSFs after interviewing 20 participants. Hence, we concluded that interviewing 32 participants for this phase of the study was sufficient. The CSFs and what they entailed are described next.

Executive Management Support

During the interviews, the role of *executive management support* as a CSF with respect to the SRM implementation became clear. Management routinely carried out risk assessments of each business division. Staff considered this relevant to SRM effectiveness because it gave everyone the impression that risk assessments should be taken seriously at all organizational levels.

Organizational Maturity

Before carrying out a risk assessment in a business division, the security management team conducted an audit of the way things were presently being done. According to senior staff members, this could shed light on some security protocols that might have been "forgotten with time." Examples included authorization and authentication processes, disaster recovery, physical security, and intrusion detection and incident response. A focus on current methods with respect to existing policies forms a core component of *organization maturity.*

Open Communication

Company A's security assessment team used tables, questionnaires, and standard report forms to facilitate the functioning of its SRM program. Employees who participated in the risk assessments were familiar with these tools, which facilitated effective communication of results of the various risk assessments. The employees also stated that the extensive use of this simple method of open communication increased understanding of SRM objectives between management, system support staff, and security specialists.

Risk Management Stakeholders

It is interesting to note that Company A relied exclusively on in-house personnel instead of an outside contractor to carry out risk assessments of their SRM program. According to a

lower level manager, this was necessitated by the nature of their work and the risks involved in the event the contractor leaked sensitive information about some of the company's programs.

Employees selected to carry out the risk assessments were well aware of the entire SRM program. This is in line with the description of what constitutes the definition of risk management stakeholders. According to management, use of in-house employees for this purpose better enabled them to explore a greater variety of risks.

Team Member Empowerment

Each business division was empowered to request a test of the SRM program via an assessment. The responsibility of following up on resulting recommendations also lied primarily with the requesting division. According to an executive manager, each business division was best qualified to determine when an assessment was required and to ensure that recommendations for risk reduction techniques resulting from the assessment were implemented effectively.

Holistic View of an Organization

Groups and individuals were designated as focal points to oversee the various risk assessment processes. Due to the overarching nature of Company A's SRM implementation, it was necessary that these groups and individuals had a clear view of the effectiveness of the SRM program. According to management, this facilitated the performance, planning, and reporting associated with Company A's SRM program, and ensured that enterprise wide issues were appropriately addressed.

Security Maintenance

Security maintenance is defined as a set of controls and best practices, such as policy updates, access control, and physical and personnel security that organizations should adopt to

maintain a sufficient security standard (Dhillon 2007). This CSF entails many of the security features that form the backbone of Company A's SRM program. Features include role-based access control, encryption standards, physical security, and policy updates. An interesting feature of this control is that if employees wish to view any of the security bulletins they can only access information that may pertain to them in their current capacity. According to one of the participants interviewed, this allowed for "removal of unnecessary clutter, and motivates most to read the policy [in the first place]."

The primary focus on encryption standards pertained to company laptops that most employees took home with them. Each laptop had full disk encryption that used Trusted Platform Module (TPM) technology. This was implemented after a security incident involving a lost laptop. Company A's site had a high degree of physical security. Visitors were not allowed to enter the premises without an escort. They had to first pass through a scanner. Next, they were physically searched by a guard. Company A employees only had to pass through the scanner but were randomly asked to volunteer for a physical search. Also, all lobbies, corridors, and common areas such as the cafeteria had closed circuit television monitoring.

Both management and staff as a major area of concern repeatedly mentioned policy updates. Although they agreed that this was a CSF, 19 of the 32 employees interviewed expressed concerns about the lack of security bulletin updates. Some of the bulletins had not been updated in almost six years. According to one employee, the lack of updated compliance guidelines could pose threats such as "covert downloads of a Trojan, malicious employee attacks, use of insecure cloud computing applications, and botnets."

Corporate Security Strategy

Corporate security strategy is defined as steps such as development of technologies undertaken by management to incorporate security needs as a fundamental function of the corporation (Dhillon 2007). As previously stated, management focused on bridging the gap between U.S. and EU regulatory compliances to assure that all regulations and requirements were satisfied. These regulations, in addition to Company A's own security standards, called for establishment of tailor-made procedures and protocols that integrated the disparate requirements. Company A encouraged the creation of cutting-edge technologies and considered it as one of the cornerstones of its SRM program. Staff members agreed with the importance of in-house security software and its role in providing an effective SRM program.

Human Resource Development

Human resource development is defined as the existence of a company framework that focuses on development of personal and organizational skills, knowledge, and abilities. With respect to SRM at Company A, this could include opportunities such as employee risk and security training. This could be quantified through focus on various security certifications such as Certified Information Systems Security Professional (CISSP) and Certified Information Systems Auditor (CISA) (Dhillon 2007). Staff members expressed an interest in knowing the background knowledge and experience of personnel who dealt with security related issues. The reason for their concern pertained to privacy and confidentially. Management stated that although "extensive logical and technical controls exist[ed], personnel experience was just as important as the other aspects." They felt that in order to reduce human error, fraud, or misuse of company property, those in charge of the process had to be carefully screened and mandated to go through education and training.

Ranking of CSFs

We asked the participants to rank the CSFs according to their perceived importance using Q-sort. This technique has been recommended in previous studies (Stephenson 1953). As part of this method each employee was given a set of cards, each of which had a CSF. They were then asked to arrange the cards in order of perceived significance (from highest to lowest). The ranking provided us with more information with regard to employee preferences based on their own subjective scale. Results are presented in Table 3 in order of decreasing importance of each management level and staff. A total of 40 employee participated in the Q-sort exercise, which included all 32 or the interviewees and 8 more subjects who participated in the survey.

Table 3: Q-Sort Results

Rank	Executive Management	Middle Management	Lower Management	Staff
1	Executive management support	Executive management support	Executive management support	Open communication
2	Open communication	Open communication	Open communication	Executive management support
3	Holistic view of organization	Corporate security strategy	Risk management stakeholders	Risk management stakeholders
4	Corporate security strategy	Risk management stakeholders	Holistic view of organization	Corporate security strategy
5	Organization maturity	Holistic view of organization	Human resource development	Holistic view of organization
6	Human resource development	Organization maturity	Corporate security strategy	Human resource development
7	Risk management stakeholders	Security maintenance	Organization maturity	Team member empowerment
8	Security maintenance	Team member empowerment	Security maintenance	Organization maturity
9	Team member empowerment	Human resource development	Team member empowerment	Security maintenance

It is interesting to note that *executive management support* is considered the most important CSF by all management layers (executive, middle, and lower), whereas staff considers *open communication* to be the most important. Most of the CSFs in each column are fairly close

to each other in terms of rank. For example, team member empowerment appears toward the lower half of each of the rankings.

Quantitative Results for Company A

In order to gauge differences in management and staff's perception of the effectiveness of SRM policies and practices, we administered a multi-item questionnaire, based on the synthesized list of CSFs, to both management and staff. Participation was voluntary. Participants were given the option of completing either an electronic or paper based survey.

A portion of the questionnaire used to measure the CSFs was pre-validated by Kotulic (2001). Kotulic measured perceived effectiveness of an SRM program using a questionnaire that was structured for a case study. Hence, it was appropriate for our study. Each construct had multiple items associated with it in the questionnaire, each representing a CSF. Perception of SRM effectiveness was also a part of the questionnaire. As a means of minimizing response bias caused by boredom or fatigue, no more than five items per construct were presented (Schriesheim and Eisenbach 1995). However since not all CSF constructs were represented in Kotulic's initial survey, we added new items prior to validation and reliability testing. Appendix A presents the entire questionnaire.

Validity and Reliability

We asked 7 professors and 11 doctoral students at a large North-Eastern university to review the updated questionnaire. We also asked a security manager at Company A to ascertain if the questions were appropriate for each construct. This assisted in enhancing the construct validity of the questionnaire, as specified by Nunnally and Bernstein (1994). We made minor refinements to the survey and administered it to 135 employees of Company A to test for reliability and construct validity.

We used Confirmatory Factor Analysis to gauge construct validity. The results of the cross-loadings are presented in Table 4. The constructs are coded as follows: SRM effectiveness (SRM), executive management support (EMS), organization maturity (OM), open communication (OC), risk management stakeholders (RMS), team member empowerment (TME), holistic view of organization (HVO), security maintenance (SM), corporate security strategy (CSS), and human resource development (HRD).

Table 4: Cross Loadings

Constructs	Question Items	SRM	EMS	OM	OC	RMS	TME	HVO	SM	CSS	HRD
SRM	SRM-1	**0.78**	0.30	0.58	0.43	0.40	0.42	0.44	0.31	0.23	0.22
	SRM-2	**0.68**	0.31	0.36	0.28	0.42	0.41	0.49	0.26	0.22	0.20
	SRM-3	**0.78**	0.37	0.48	0.43	0.40	0.46	0.54	0.22	0.31	0.24
	SRM-4	**0.72**	0.44	0.13	0.46	0.43	0.34	0.54	0.26	0.43	0.27
	SRM-5	**0.76**	0.34	0.40	0.53	0.29	0.51	0.58	0.37	0.22	0.20
EMS	EMS-1	0.39	**0.79**	0.10	0.44	0.20	0.26	0.47	0.15	0.12	0.31
	EMS-2	0.54	**0.80**	0.18	0.47	0.16	0.56	0.14	0.36	0.25	0.37
	EMS-3	0.56	**0.81**	0.12	0.51	0.55	0.49	0.27	0.35	0.55	0.34
OM	OM-1	0.48	0.41	**0.91**	0.38	0.36	0.55	0.20	0.39	0.57	0.31
	OM-2	0.43	0.42	**0.90**	0.33	0.15	0.46	0.31	0.31	0.25	0.38
	OM-3	0.10	0.22	**0.89**	0.30	0.36	0.49	0.37	0.26	0.22	0.46
OC	OC-1	0.10	0.41	0.50	**0.69**	0.18	0.29	0.14	0.22	0.31	0.39
	OC-2	0.38	0.34	0.52	**0.66**	0.19	0.26	0.31	0.26	0.14	0.36
RMS	RMS-1	0.29	0.30	0.50	0.12	**0.79**	0.29	0.28	0.37	0.11	0.33
	RMS-2	0.48	0.43	0.33	0.10	**0.87**	0.27	0.36	0.15	0.29	0.38
TME	TME-1	0.46	0.41	0.19	0.04	0.04	**0.78**	0.39	0.36	0.19	0.32
	TME-2	0.38	0.53	0.30	0.17	0.17	**0.62**	0.36	0.35	0.15	0.44
	TME-3	0.53	0.34	0.36	0.10	0.10	**0.69**	0.19	0.39	0.09	0.12
	TME-4	0.50	0.10	0.35	0.21	0.21	**0.79**	0.17	0.54	0.10	0.14
HVO	HVO-1	0.40	0.19	0.46	0.27	0.27	0.11	**0.69**	0.31	0.41	0.31
	HVO-2	0.28	0.20	0.25	0.44	0.44	0.10	**0.76**	0.21	0.55	0.24
SM	SM-1	0.22	0.44	0.46	0.11	0.11	0.14	0.29	**0.68**	0.22	0.21
	SM-2	0.32	0.41	0.58	0.18	0.18	0.11	0.48	**0.71**	0.42	0.29
CSS	CSS-1	0.34	0.55	0.53	0.16	0.16	0.35	0.51	0.30	**0.91**	0.11
	CSS-2	0.49	0.32	0.20	0.19	0.19	0.22	0.53	0.29	**0.95**	0.19
HRD	HRD-1	0.35	0.21	0.40	0.46	0.46	0.31	0.56	0.13	0.47	**0.80**
	HRD-2	0.43	0.29	0.48	0.53	0.53	0.39	0.52	0.12	0.52	**0.75**

As shown, the factor loadings are all above the suggested threshold of 0.6 (Chin 1998). In addition, items that measure the same construct have higher loadings than those measuring other constructs. This suggests acceptable convergent and discriminant validity. To further assess construct validity, Table 5 presents the correlation between the constructs, with the diagonal elements being the square root of the average variance extracted (AVE). The AVE of each construct exceeded 0.5, the benchmark for convergent validity (Fornell and Larcker 1981). In addition, the square root of the AVE of each construct was greater than the correlation between the construct and other constructs, suggesting adequate discriminant validity.

Table 5: Correlations and Square Root of AVE

Constructs	SRM	EMS	OM	OC	RMS	TME	HVO	SM	CSS	HRD
SRM	0.78									
EMS	0.45	0.74								
OM	0.26	0.35	0.80							
OC	0.33	0.39	0.19	0.65						
RMS	0.47	0.32	0.20	0.32	0.70					
TME	0.51	0.31	0.13	0.17	0.36	0.76				
HVO	0.42	0.40	0.44	0.19	0.45	0.20	0.62			
SM	0.39	0.51	0.38	0.21	0.43	0.34	0.23	0.81		
CSS	0.27	0.54	0.23	0.18	0.26	0.11	0.28	0.39	0.80	
HRD	0.44	0.12	0.17	0.11	0.32	0.19	0.30	0.47	0.41	0.83

The reliability was assessed using Cronbach's alpha and composite reliability. Table 6 shows that the alpha value and composite reliability for each construct was above 0.7, the suggested threshold for adequate reliability (Nunnally and Bernstein 1994).

Table 6: Reliability Analysis

Constructs	Cronbach's Alpha	Composite Reliability
SRME (5 items)	0.80	0.91
EMS (3 items)	0.76	0.90
OM (3 items)	0.78	0.88
OC (2 items)	0.74	0.89
RMS (2 items)	0.81	0.88
TME (4 items)	0.82	0.76
HVO (2 items)	0.80	0.79
SM (2 items)	0.79	0.82
CSS (2 items)	0.75	0.75
HRD (2 items)	0.72	0.77

Once we ascertained the reliability and validity, we administered the survey (either electronic or paper version) to the rest of the employees at Company A. The next section provides the quantitative results from the participants of the study.

RESULTS

A total of 272 out of 378 employees, excluding those who participated in the pilot study, took part in the survey portion of the study at Company A. Hence, the response rate was 71.96%. Table 7 provides statistics on the total number of participants, along with demographic information.

Table 7: Employee Demographics (Company A)

Employee Level	# Surveyed	Average Age	Education		
			Bachelors	Masters	Doctorate
Executive Mgt.	15	51.73	2	12	1
Middle Mgt.	22	44.00	6	16	
Lower Mgt.	50	38.08	12	35	3
Staff	185	31.81	142	43	
Total	272	N/A	162	106	4

We compared the management layers (executive, middle, and lower) with the staff to measure differences in perception in the effectiveness of current SRM policies and practices. In

each case, we established linear regression models with dummy variables with interaction effects. The independent variables are the nine CSFs along with dummy regressors for management and staff. The dependent variable is SRM effectiveness. Using the data, we carried out different levels of data analyses with regard to one of the purposes of this study: identify CSFs that may highlight differences in perceptions of SRM effectiveness among management and staff.

We checked and corrected for violation of any of the OLS assumptions. We also checked for heteroskedasticity using the Breusch-Pagan (BP) test (1979). If the BP test was significant, indicating inefficient OLS, we used Generalized Least Squares (GLS) estimators.

Considering that there were a limited number of executive and middle managers, it was more prudent to incorporate one interaction effect per layer and compare two groups at a time. By concentrating on the interaction effect, we were able to gauge the perceptions of employees at different levels on each CSF and its impact on SRM effectiveness. This resulted in 54 multiple regression equations. A general form of the regression equation used was:

$$SRM = \beta_0+\beta_1 EMS +\beta_2 OM+ \beta_3 OC+ \beta_4 RMS+ \beta_5 TME+\beta_6 HVO+\beta_7 SM+\beta_8 CSS+\beta_9 HRD + \delta_1 Layer + X_1 CSF*LAYER +\varepsilon \quad (1)$$

Where

Layer=Executive management (EM), Middle management (MM), Lower management (LM), or Staff (ST)

CSF=EMS, OM, OC, RMS, TME, HVO, SM, CSS, or HRM

Executive Management (EM) and Middle Management (MM)

To gauge the differences in perception between executive management and middle management with regard to how each CSF influences current perceived SRM effectiveness, we

used equation (1). EM was "0" in the event a person belonged to middle management and "1" if the employee belonged to executive management.

Since the focus was on the interaction term, the tabulated results that follow only provide the relevant regression coefficients. Table 8 provides results when considering each CSF as an interaction term.

The results presented in the proceeding tables refer to a different regression for each CSF. Since we compared two groups for each regression, the critical value was the interaction between the CSF and the binary variable for the group.

Table 8: EM and MM – Interactions with Each CSF

	OLS		**BP Test Significant?**	**GLS**	
Coefficients	**Estimate**	**Adj. R^2**		**Estimate**	**Adj. R^2**
EMS x **EM**	0.74***	0.70	No	NA	NA
OM x **EM**	0.17	0.50	Yes	0.23**	0.94
OC x **EM**	0.29*	0.55	Yes	0.31***	0.89
RMS x **EM**	-0.83***	0.61	Yes	-0.78***	0.88
TME x **EM**	-0.10	0.49	Yes	-0.23***	0.83
HVO x **EM**	-0.20	0.51	Yes	-0.11*	0.98
SM x **EM**	0.24	0.54	Yes	0.14**	0.98
CSS x **EM**	-0.98***	0.73	Yes	-1.11***	0.95
HRD x **EM**	0.46	0.54	Yes	0.60***	0.95

*** $p < 0.01$; ** $p < 0.05$; * $p < 0.10$

As shown, executive and middle management differ significantly in terms of perceived effectiveness of SRM policies and procedures, as related to all nine of the CSFs. Overall, executive management has more positive perceptions of the effectiveness of policies and practices related to executive management support (EMS), organizational maturity (OM), open communication (OC), security maintenance (SM), and human resource development (HRD). Conversely, they had less positive perceptions of the effectiveness of policies and practices

related to risk management stakeholders (RMS), team member empowerment (TME), holistic view of the organization (HVO), and corporate security strategy (CSS).

Executive Management (EM) and Lower Management (LM)

None of the CSFs was significant (Table 9). Hence, there was no significant difference in perception between executive and lower management with regard to the CSFs pertaining to SRM effectiveness.

Table 9: EM and LM – Interactions with Each CSF

	OLS		BP Test Significant?	GLS	
Coefficients	**Estimate**	**Adj. R^2**		**Estimate**	**Adj. R^2**
EMS x **EM**	-0.04	0.82	No	NA	NA
OM x **EM**	-0.01	0.82	No	NA	NA
OC x **EM**	0.12	0.81	No	NA	NA
RMS x **EM**	-0.04	0.79	No	NA	NA
TME x **EM**	-0.03	0.77	No	NA	NA
HVO x **EM**	-0.07	0.80	No	NA	NA
SM x **EM**	-0.08	0.82	No	NA	NA
CSS x **EM**	-0.17	0.82	No	NA	NA
HRD x **EM**	0.07	0.82	No	NA	NA

*** $p < 0.01$; ** $p < 0.05$; * $p < 0.10$

Executive Management (EM) and Staff (ST)

Although there was no significant difference in perceptions of SRM effectiveness between executive and lower management (Table 9), executive management and staff differed for each CSF (Table 10). In each instance, executive management has a less positive view than staff regarding the effectiveness of the current SRM policies and procedures, as related to the CSFs although it is not statistically significant.

Table 10: EM and ST – Interactions with Each CSF

	OLS		BP Test Significant?	GLS	
Coefficients	**Estimate**	**Adj. R^2**		**Estimate**	**Adj. R^2**
EMS x **EM**	0.01	0.80	Yes	-0.13***	0.99
OM x **EM**	-0.20	0.80	Yes	-0.21***	0.97
OC x **EM**	-0.02	0.79	Yes	-0.08**	0.99
RMS x **EM**	-0.50	0.80	Yes	-0.53***	0.99
TME x **EM**	-0.13	0.80	Yes	-0.15***	0.93
HVO x **EM**	-0.24	0.79	Yes	-0.23***	0.99
SM x **EM**	0.01	0.79	Yes	-0.12***	0.99
CSS x **EM**	-0.63	0.80	Yes	-0.43***	0.99
HRD x **EM**	-0.17	0.80	Yes	-0.20***	0.99

*** p < 0.01; ** p < 0.05; * p < 0.10

Middle Management (MM) and Lower Management (LM)

Table 11 shows results for the model when the interaction terms for each CSF are included. The results were significant for the EMS, OC, TME, HVO and SM interactions. Overall, middle management perceives the effectiveness of SRM policies and practices related to TME and HVO more positively than does lower management. Conversely, they have less positive perceptions of the effectiveness of SRM policies and practices related to EMS, OC, and SM.

Table 11: MM and LM – Interactions with Each CSF

	OLS		BP Test Significant?	GLS	
Coefficients	**Estimate**	**Adj. R^2**		**Estimate**	**Adj. R^2**
EMS x **MM**	-0.65***	0.76	No	NA	NA
OM x **MM**	-0.10	0.70	No	NA	NA
OC x **MM**	-0.26**	0.72	No	NA	NA
RMS x **MM**	-0.06	0.70	No	NA	NA
TME x **MM**	0.05	0.70	Yes	0.10***	0.96
HVO x **MM**	0.04	0.70	Yes	0.25**	0.96
SM x **MM**	-0.31**	0.71	No	NA	NA
CSS x **MM**	-0.06	0.70	No	NA	NA
HRD x **MM**	-0.02	0.70	No	NA	NA

*** p < 0.01; ** p < 0.05; * p < 0.10

Middle Management (MM) and Staff (ST)

Table 12 compares interaction terms between middle management and staff. As shown, middle management has less positive perceptions than staff in reference to the effectiveness of SRM policies and practices related to EMS, RMS, SM, CSS, and HRD.

Table 12: MM and ST – Interactions with Each CSF

	OLS		BP Test Significant?	GLS	
Coefficients	**Estimate**	**Adj. R^2**		**Estimate**	**Adj. R^2**
EMS x **MM**	-0.13	0.79	Yes	-0.20***	0.99
OM x **MM**	-0.02	0.79	No	NA	NA
OC x **MM**	-0.08	0.79	No	NA	NA
RMS x **MM**	-0.13	0.79	Yes	-0.10***	0.99
TME x **MM**	-0.05	0.79	No	NA	NA
HVO x **MM**	-0.03	0.79	No	NA	NA
SM x **MM**	-0.22	0.79	Yes	-0.15***	0.98
CSS x **MM**	-0.11	0.79	Yes	-0.10***	0.98
HRD x **MM**	-0.21*	0.79	Yes	-0.17***	0.98

*** p < 0.01; ** p < 0.05; * p < 0.10

Lower Management (LM) and Staff (ST)

Table 13 compares interaction terms between lower management and staff. As shown, there are significant differences in seven of the nine CSFs. Lower management has a more positive perception of the effectiveness of EMS, but has less positive perceptions of the effectiveness of OM, OC, HVO, SM, CSS, and HRD.

Table 13: LM and ST – Interactions with Each CSF

	OLS		BP Test Significant?	GLS	
Coefficients	**Estimate**	**Adj. R^2**		**Estimate**	**Adj. R^2**
EMS x **LM**	0.77***	0.82	No	NA	NA
OM x **LM**	-0.07	0.82	Yes	-0.03**	0.99
OC x **LM**	-0.05	0.82	Yes	-0.05***	0.99
RMS x **LM**	-0.04	0.82	No	NA	NA
TME x **LM**	-0.10	0.82	No	NA	NA
HVO x **LM**	-0.17	0.82	Yes	-0.17***	0.99
SM x **LM**	-0.09	0.82	Yes	-0.11**	0.99
CSS x **LM**	-0.07	0.82	Yes	-0.04*	0.99
HRD x **LM**	-0.14	0.82	Yes	-0.10***	0.99

*** $p < 0.01$; ** $p < 0.05$; * $p < 0.10$

Quantitative Results for Company B

As previously stated, both Company A and Company B are Fortune 500 technology companies. As such, Company B was selected to determine if both firms agreed in reference to the CSFs and their impact on SRM effectiveness.

We administered the same questionnaire to full time employees at one of the locations of Company B. One hundred fifteen (115) out of 132 personnel at Company B responded to the survey. Hence, the response rate was 87.12%. Table 14 presents participant demographics.

Table 14: Employee Demographics

Employee Level	**# Surveyed**	**Average Age**	**Education**		
			Bachelors	**Masters**	**Doctorate**
Executive Mgt.	3	54.21		3	
Middle Mgt.	10	49.50	3	7	
Lower Mgt.	23	34.14	10	12	1
Staff	79	28.26	65	14	
Total	115	N/A	78	36	1

To analyze the survey results, we used the same regression modeling technique employed for Company A. The following sections present the perception of SRM effectiveness at Company B. We included Company A results for each regression analysis for comparison.

Executive Management (EM) and Middle Management (MM)

Significant interactions existed for EMS, OM, OC, RMS, TME, and HVO (Table 15). Company B's executive management is less positive than middle management in reference to HVO. All other significant interactions indicated that their perceptions toward SRM effectiveness related to these CSFs were positive.

Table 15: EM and MM – Interactions with Each CSF

	Company B		**Company A**	
	OLS		**OLS/GLS**	
Coefficients	**Est.**	**Adj. R^2**	**Est.**	**Adj. R^2**
EMS x **EM**	0.48^{***}	0.60	0.74^{***}	0.70
OM x **EM**	0.21^{*}	0.41	0.23^{**}	0.94
OC x **EM**	0.47^{**}	0.39	0.31^{***}	0.89
RMS x **EM**	0.14^{***}	0.50	-0.78^{***}	0.88
TME x **EM**	0.42^{***}	0.69	-0.23^{***}	0.83
HVO x **EM**	-0.10^{***}	0.30	-0.11^{*}	0.98
SM x **EM**	0.01	0.74	0.14^{**}	0.98
CSS x **EM**	0.61	0.68	-1.11^{***}	0.95
HRD x **EM**	0.14	0.66	0.60^{***}	0.95

*** p < 0.01; ** p < 0.05; * p < 0.10

Executive Management (EM) and Lower Management (LM)

Table 16 compares interaction terms between executive and lower management. As shown, executive management has more positive perceptions regarding the effectiveness of their SRM policies and practices related to EMS, OM, and HRD. All other interactions were not significant. As shown, there were no significant differences between Company A's executive and lower management.

Table 16: EM and LM – Interactions with Each CSF

	Company B		Company A	
	OLS		OLS/GLS	
Coefficients	**Est.**	**Adj. R^2**	**Est.**	**Adj. R^2**
EMS x **EM**	0.15**	0.64	-0.04	0.82
OM x **EM**	0.22**	0.61	-0.01	0.82
OC x **EM**	0.04	0.56	0.12	0.81
RMS x **EM**	0.02	0.54	-0.04	0.79
TME x **EM**	0.14	0.39	-0.03	0.77
HVO x **EM**	-0.19	0.67	-0.07	0.80
SM x **EM**	0.19	0.61	-0.08	0.82
CSS x **EM**	0.10	0.29	-0.17	0.82
HRD x **EM**	0.14*	0.32	0.07	0.82

*** p < 0.01; ** p < 0.05; * p < 0.10

Executive Management (EM) and Staff (ST)

Table 17 compares interaction terms between executive management and staff. Interestingly, these results are very different from those of Company A. Whereas Company A's executive management had less positive perceptions regarding all nine CSFs, Company B's executive management was either more positive (EMS, OM, OC, SM, and CSS), or results were not significant.

Table 17: EM and ST – Interactions with Each CSF

	Company B		Company A	
	OLS		OLS/GLS	
Coefficients	**Est.**	**Adj. R^2**	**Est.**	**Adj. R^2**
EMS x **EM**	0.21***	0.61	-0.13***	0.99
OM x **EM**	0.31**	0.62	-0.21***	0.97
OC x **EM**	0.19**	0.45	-0.08***	0.99
RMS x **EM**	0.19	0.58	-0.53***	0.99
TME x **EM**	0.32	0.61	-0.15***	0.93
HVO x **EM**	0.29	0.33	-0.23***	0.99
SM x **EM**	0.09*	0.53	-0.12***	0.99
CSS x **EM**	0.01*	0.52	-0.43***	0.99
HRD x **EM**	0.03	0.60	-0.20***	0.99

*** p < 0.01; ** p < 0.05; * p < 0.10

Middle Management (MM) and Lower Management (LM)

When compared to lower management (Table 18), middle management considers EMS, OM, OC, CSS, and HRD to have a more positive impact on SRM effectiveness. Once again, this is in contrast to Company A.

Table 18: MM and LM – Interactions with Each CSF

	Company B		**Company A**	
	OLS		**OLS/GLS**	
Coefficients	**Est.**	**Adj. R^2**	**Est.**	**Adj. R^2**
EMS x **MM**	0.31***	0.60	-0.65***	0.76
OM x **MM**	0.41***	0.51	-0.10	0.70
OC x **MM**	0.21**	0.49	-0.26**	0.72
RMS x **MM**	0.19	0.61	-0.06	0.70
TME x **MM**	0.21	0.53	0.10***	0.96
HVO x **MM**	0.18	0.49	0.25**	0.96
SM x **MM**	0.19	0.50	-0.31**	0.71
CSS x **MM**	0.11**	0.61	-0.06	0.70
HRD x **MM**	0.29**	0.61	-0.02	0.70

*** $p < 0.01$; ** $p < 0.05$; * $p < 0.10$

Middle Management (MM) and Staff (ST)

Table 19 shows that all interactions between middle management and staff were significant. For each CSF, middle management has a more positive perception of the effectiveness of SRM policies and practices. These results are quite different from those of Company A. Although not statistically significant in all instances, Company A's middle management considers each of the CSFs to have a less positive impact on SRM effectiveness when compared to staff.

Table 19: MM and ST – Interactions with Each CSF

	Company B		Company A	
	OLS		OLS/GLS	
Coefficients	**Est.**	**Adj. R^2**	**Est.**	**Adj. R^2**
EMS x **MM**	0.51**	0.61	-0.20***	0.99
OM x **MM**	0.32**	0.50	-0.02	0.79
OC x **MM**	0.20**	0.41	-0.08	0.79
RMS x **MM**	0.21**	0.50	-0.10***	0.99
TME x **MM**	0.11***	0.52	-0.05	0.79
HVO x **MM**	0.02**	0.51	-0.03	0.79
SM x **MM**	0.39**	0.51	-0.15***	0.98
CSS x **MM**	0.19**	0.61	-0.10***	0.98
HRD x **MM**	0.31***	0.60	-0.17***	0.98

*** p < 0.01; ** p < 0.05; * p < 0.10

Lower Management (LM) and Staff (ST)

As shown in Table 20, when comparing lower management to staff at Company B, all CSFs were significant and positive. Once again, these results differ from those of Company A. Overall, Company A's lower management is less positive than staff in reference to the CSF impact on SRM effectiveness.

Table 20: LM and ST – Interactions with Each CSF

	Company B		Company A	
	OLS		OLS/GLS	
Coefficients	**Est.**	**Adj. R^2**	**Est.**	**Adj. R^2**
EMS x **LM**	0.31**	0.60	0.77***	0.82
OM x **LM**	0.12**	0.51	-0.03**	0.99
OC x **LM**	0.30***	0.55	-0.05***	0.99
RMS x **LM**	0.30***	0.60	-0.04	0.82
TME x **LM**	0.22***	0.61	-0.10	0.82
HVO x **LM**	0.51**	0.59	-0.17***	0.99
SM x **LM**	0.21**	0.69	-0.11**	0.99
CSS x **LM**	0.31***	0.45	-0.04*	0.99
HRD x **LM**	0.29***	0.55	-0.10***	0.99

*** p < 0.01; ** p < 0.05; * p < 0.10

DISCUSSION OF RESULTS: COMPANIES A AND B

Management and staff of Company B differ significantly from those of Company A in terms of their perceived effectiveness of SRM policies and practices, as related to each of the nine CSFs. In company A, management tended to have less positive perceptions of the effectiveness of SRM policies, as related to each of the nine CSFs. Conversely, Company B's executive management tended to be more positive than staff or other levels of management. Although we extracted the CSFs from interviews with Company A, Company B tended to agree with their significance. The results also show that in Company B, management and staff predominantly agree on the current CSF implementations, and have a positive perception about their impact on SRM effectiveness. This is different from Company A. Some of the CSFs are not perceived as effectively being met by the current SRM policies and practices.

We ran an additional regression test for each of the two firms, comparing all layers of management with that of staff. This ascertained macro-level differences with regard to the impact of the CSFs on perceived SRM effectiveness. The regression equation was:

$$SRM = \beta_0 + \beta_1 EMS + \beta_2 OM + \beta_3 OC + \beta_4 RMS + \beta_5 TME + \beta_6 HVO + \beta_7 SM + \beta_8 CSS + \beta_9 HRD + \delta_1 MGT + \varepsilon \quad (2)$$

Where, the dummy value MGT was "1" if an employee was a part of any of the management layers, and "0" otherwise (staff).

Table 21 shows the results for both companies

Table 21: Combined Management Layer against Staff - Companies A and B

	Company A	Company B
	GLS (Adj. R^2: 0.99)	OLS (Adj. R^2: 0.52)
Coefficients	**Estimate**	**Estimate**
EMS	0.40***	0.51***
OM	0.10***	0.14**
OC	0.18***	0.25**
RMS	-0.12***	0.04**
TME	-0.13***	0.20**
HVO	0.23***	0.10**
SM	-0.06***	0.19**
CSS	0.09***	0.17**
HRD	0.16***	0.02**
MGT	-0.43***	0.31***

*** p < 0.01; ** p < 0.05; * p < 0.10

Unlike the previous regression models in which the focus was on individual interactions between a CSF and a group, results from equation 2 have to be interpreted as a whole. Hence its macro-level description quality. For Company A, the negative coefficients for RMS, TME, and SM, and MGT imply that neither management nor staff is satisfied with the current policies and practices with respect to the three CSFs. Conversely, at Company B, management and staff have a positive perception about all CSFs and their impact on SRM effectiveness.

Table 21 shows that at Companies A and B, each group considered each of the CSFs important for SRM effectiveness. However, they varied on the degree the CSFs impacted current perceived SRM effectiveness. This mirrored results from the previous regression models.

From the interviews with employees of Company A, we found additional information related to risk management stakeholders, team member empowerment, and security maintenance. The next section provides a discussion of these CSFs.

Qualitative Discussion of Company A

In the area of risk management stakeholders, we previously mentioned that Company A selected a certain number of its own employees to carry out risk assessments in business divisions. Both management and staff agree to the overall goals such as exposing employees to gain experience by carrying out tasks pertaining to risk assessment, but they disagree on some of the reasons behind them. For example, management is concerned about the possibility of an intruder from outside the firm getting unrestricted access under the umbrella of a risk assessor. Staff, on the other hand, feels that a management employee who has been with Company A for a long time and has unrestricted access to most resources could be a prime candidate for an insider threat. There is theoretical support with regard to the seriousness of threats posed by insiders (Stanton et al. 2005). A staff employee presented an interesting opinion. According to this employee, "if you have a large company, some may be dishonest. But we've had compromises because of a failure to trust insiders. Those who set up the network hold a lot of power, and are smart enough to quietly move sensitive data off a network. But we trust them, some of whom are longtime employees. I differentiate between people trying to protect systems." A lower level manager partially agreed with this assessment. "Large organizations like ours have different problems. A person with plenty of experience and [who] is well compensated is a low risk. It is unlikely that he is malicious, but it is certainly possible."

These comments show that management and staff are seemingly aware of potential insider threats. Both management and staff implied that trust is a factor in allowing access to company resources, but trust is not a security policy. By the staff member's own argument, privileged account abuse could occur. We suggest that management include privileged identities within the broader Identity Management project scope (Fyffe 2008). This is important because if

privileged access is not included in the initial scope, they will probably not address it. We suggest that Company A identify key systems and applications. Current applications in the organization have underlying generic identities, which, once accessed through a privileged account could provide wide-ranging access to other company applications. We also suggest Company A monitor and report actual adherence to the set policies (Magklaras and Furnell 2005). It is not sufficient to simply know who is accessing privileged accounts. They should monitor account activity once access is granted to ensure that the activity itself is compliant with the organization's security and business policies.

Team member empowerment is linked to risk management stakeholders. As previously stated, a division is empowered to independently request a risk assessment. However, the request can only be made by a division manager. Management contended that while insiders posed a legitimate threat, those instances were rare. However, staff indicated that they prefer regular assessments carried out by external parties. However, staff is also bothered by the fact that such decisions are cost-driven, and their own concerns are not addressed. Staff does not doubt management's competency, but believes management is unwilling to permit risk assessments based on a staff member's recommendation. We suggest that management consider expanding the manner in which they handle assessment requests. Staff employees prefer suggestion boxes and other employer based mechanisms that would give them individual access to management. It may also serve management well if some type of a joint SRM committee represented by staff and management alike is set up. Also, to preserve a sense of neutrality, Company A should alter the method of carrying out risk assessments (Calder 2006). Currently, personnel for risk assessments are selected from the division that requests a risk assessment. This is based on employee familiarity with how the division worked. Requiring personnel from other divisions to perform

risk assessments will reduce the chance of compromising the quality of the assessment. Also, risk assessments are scheduled by the SRM team with the requestor. We suggest that after a request is initiated, the actual day of the risk assessment should be unknown. This may assist in countering instances of divisions erecting temporary procedures to pass the assessments and removing them once the assessment is completed.

Security maintenance is the third CSF of major concern to management and staff at Company A. This CSF was previously defined to incorporate security protocols such as policy updates, compliance, and access control. What is noteworthy is that management considers implementation of security protocols more important that does staff.

Management does not concern itself with the "how-to" portion of actual implementation of security procedures. For example, management supports development of in-house security software to comply with the set security standards, but the exact reasons for its use are not as clear to them as it is to staff. According to a staff member, "attacks and compliance failures have the same cause. A malicious insider introduces a bot in the network, and it bogs down the CPU and disks. We should not want to address a symptom (CPU overload) and miss the real problem – loss of some data (compliance failure) due to a crime. We need to fix that because at times we can't resolve the issue quickly." In a middle manager's opinion, the security team "has too many acronyms, and most of them only confuse everyone. Take for instance APT (advanced persistent threat). Do I really care about what it does? Or should I care about how I can counter it and any other acronym thrown at me?" The manager was clearly concerned with the "bigger picture". He continued, "The only counter for threats is a well thought-out security program that includes a thoughtful executive at the top, regular assessments, and quick remediation when threats are identified. And always talk about how many man-hours it would take to create the secret sauce

yourself." We suggest that Company A use external contractors that specialize in developing security tools (Calder and Watkins 2008). Company A had relationships with numerous professional organizations that it would benefit from with regard to development of security software. Currently, Company A relied on a cadre of in-house software engineers who had CISSPs or CISMs. However, that is not sufficient. These security certifications provide a landscape of general information security understanding. Organizations whose business is security software development maintain workers who have a wider arsenal of security training because they are aware of the latest technologies and threats, while also having a greater capability of countering potential future threats. This is important, because current concepts of root kits, buffer overflows, SQL injection, and cross site scripting are now commoditized into tools, and are explained in detail in publications. Therefore, the value of Company A's own software developers having knowledge about them has diminished. This does not imply that Company A should not let its own employees participate in this process. Having a joint team of external contractors and qualified internal members will provide an ideal blend. The internal members, due to their general experience in security, will be able to clearly articulate Company A's requirements to the external contractors. Having a team representing both parties will also ensure that each can "police" the other.

As part of the security maintenance CSF, we also found that some security bulletins are not updated on a timely basis. In addition to ensuring timely updates, to truly gauge if security bulletins are relevant, we suggest that Company A conduct brief simulation exercises. These can be a part of the risk assessment process. Simulating different breach scenarios at least two times a year will ensure that all employees are aware of the current action plans as specified by the current SRM program.

RESEARCH CONTRIBUTION

One of the main contributions of this research is that we were able to obtain sensitive information related to information security and risk management. In addition this is one of few studies on information security that involve Fortune 500 companies. This research confirmed six initial CSFs (executive management support, organization maturity, open communication, risk management stakeholders, team member empowerment, and holistic view of organization) and discovered three new CSFs (security maintenance, corporate security strategy, and human resource development). Each of these CSFs had an underlying theme - a congruence of SRM program objectives and policies that would make them effective. The use of a widely-recognized theory from organizational studies in a case study environment allowed greater focus on the roles that levels of management and staff play with regard to SRM effectiveness. We used a combination of qualitative and quantitative methods to validate the finding. The impact of roles was quantified through multiple regression models with and without interaction effects.

This study also contributes to the CSF literature by applying the CSF method across not only layers of management, as has been done in previous studies, but also the staff layer. SRM implementations in organizations are complex and enterprise-wide. Therefore, for an effective SRM program, all stakeholders should be considered.

IMPLICATIONS FOR ACADEMICIANS AND PRACTICE

For academicians, this study shows that the CSF method can be modified to address complex organizational issues such as SRM effectiveness. As stated throughout this paper, information security research at the organizational level has constantly faced challenges due to its intrusive nature. In most cases, management approval is needed to carry out research of such

magnitude. The CSF method is a management-friendly form of research. It allows for the use of structured and unstructured dialogue with the added opportunity of the researcher communicating CSFs back to management for approval. This method, if explained properly to management, has the potential to deter many of the fears associated with information security related research.

Recognizing that differences in perception exist among layers of management and staff in terms of SRM effectiveness is a vital issue that needs to be addressed by the security management team. In Company A, through results from the q-sort exercise and multiple regression models, we found that certain CSFs such as executive management support ranked consistently higher than the rest. Staff considered executive management to be the prime mover behind SRM effectiveness. Based on the observations, it is obvious that the current SRM implementation at Company A does have executive buy-in. However, there is a need to better communicate management's proactive role in SRM implementation to staff. Better communication channels will create synergy between different employee levels and encourage an effectiveness of the SRM program. We can link this objective to open communication and holistic view of the organization, two highly-ranked CSFs according to our results. For management to effectively communicate its SRM vision, the organization must have a network structure with clearly demarcated boundaries.

The absence of policy updates was one of the more glaring deficiencies pertaining to the current SRM implementation at Company A. Security by its nature is an evolving field. Therefore, it is important to ensure that security policies are as up-to-date as possible.

There are other potential implications as well. Inconsistent perception of CSFs on SRM effectiveness may cause liability issues. For example, problems associated with intellectual property can result in class action lawsuits as well as criminal liability. We found significant differences in perception among management and staff in reference to intellectual property.

The scenarios showed how a lack of understanding of a SRM program could deter employees from being as productive in their work as they would normally be. This loss of productivity could prove to be critical for an organization since it could result in lost revenue and/or customers.

LIMITATIONS

One of the potential limitations of this study is that it considers CSFs in the context of only two organizations. Therefore, results cannot be generalized across other companies. This limitation is somehow reduced by the fact that both companies are multinational Fortune 500 technology firms with an established security risk management program. However, due to its sensitive, complex nature, this was meant to be an exploratory study. Advances in both the science and practice of information systems and allied disciplines (e.g. management, computer science, and psychology) hinge on results derived from exploratory research. As part of role theory development, Katz and Kahn (1978) initially had more than a dozen factors derived from observed phenomena as part of exploratory research. They made it a life's work of testing those factors in different environments before settling on a core list of role theory tenets applicable to organizations. A similar path can be followed by testing the synthesized list of the CSFs found in this study across organizations in different industries.

Another potential limitation may be that the research method, albeit management-friendly, may have biased employees toward a particular CSF. Care was taken with regard to this problem via the use of standardized scripts and an overall sense of neutrality and passive role on the part of the researcher.

Finally, the issue of adequate sample size needs to be discussed, especially with regard to the total number of participants in Company B. At the estimation stage, the problem of sample size is largely removed by the use of unbiased estimators. Under random sampling, the expected value of the unbiased sample estimator will be the true parameter value, regardless of the sample size. However, as in any statistical estimation, the statistical consistency of the estimator is improved as the sample size increases. A small sample size is also not a concern in exact cases of inference where sampling distributions are either independent of the sample size or dependent upon the degree of freedom, thus explicitly incorporate the sample size. However, a small sample size could be of concern in cases of inference that rely on asymptotic sampling distributions. The regression procedures employed in this study are consistent with the small sample properties.

SUGGESTIONS FOR FUTURE RESEARCH

This exploratory work has set the stage for future research in the area of organizational information security. Future studies can include more companies of various sizes from different industries, as well as extracating additional CSFs. As shown in Company A, there were significant differences in perceptions of the effectiveness of the SRM program. Further studies should explore why these differences exist, and how problems can be resolved.

CONCLUSION

This study is the first to provide empirical evidence of the relation between CSFs and SRM effectiveness based on the perception of management and staff of two Fortune 500 companies. The study examined the differences between perceptions of management layers and staff, and found significant differences between groups based on data analysis using multiple regression models. Information security is an ongoing effort that requires regular updating on the policies as the business and regulatory requirements evolve. The qualitative part of the study found that more effective implementation of SRM can be achieved through fostering enhanced communication between layers of management and staff for greater perception alignment.

REFERENCES

Akkermans, H., and van Helden, K. 2002. "Vicious and Virtuous Cycles in Erp Implementation: A Case Study of Interrelations between Critical Success Factors," *European Journal of Information Systems* (11:1), pp 35-46.

Al-Mashari, M., and Zairi, M. 1999. "Bpr Implementation Process: An Analysis of Key Success and Failure Factors," *Business Process Management Journal* (5:1), pp 87-112.

Bandyopadhyay, T., Mookerjee, V.S., and Rao, R.C. 2009. "Why It Managers Don't Go for Cyber-Insurance Products," *Communications of the ACM* (52:11), pp 68-73.

Baroudi, J.J. 1985. "The Impact of Role Variables on Is Personnel Work Attitudes and Intentions," *MIS Quarterly* (9:4), pp 341-356.

Bayus, B.L., Erickson, G., and Jacobson, R. 2003. "The Financial Rewards of New Product Introductions in the Personal Computer Industry," *Management Science* (49:2), pp 197-210.

Bergeron, F., and Begin, C. 1989. "The Use of Critical Success Factors in Evaluation of Information Systems: A Case Study," *Journal of Management Information Systems* (5:4), pp 111-124.

Biddle, B.J., and Thomas, E.J. 1966. *Role Theory: Concepts and Research*. NY: John Wiley.

Blakley, B., McDermott, E., and Geer, D. 2001. "Information Security Is Information Risk Management," *Workshop on New Security Paradigms*, Cloudcrodt, New Mexico: ACM New York, NY, USA, pp. 97-104.

Bowman, B., Davis, G., and Wetherbe, J. 1983. "Three Stage Model of Mis Planning," *Information & Management* (6:1), pp 11-25.

Boynton, A., and Zmud, R. 1984. "An Assessment of Critical Success Factors," *Sloan Management Review (pre-1986)* (25:4), pp 17-27.

Breusch, T.S., and Pagan, A.R. 1979. "A Simple Test for Heteroscedasticity and Random Coefficient Variation," *Econometrica: Journal of the Econometric Society* (47:5), pp 1287-1294.

Bullen, C.V., and Rockart, J.F. 1981. "A Primer on Critical Success Factors," *Center for Information Systems Research* (Working Paper No. 69:Sloan School of Management), pp 1-64.

Butler, T., and Fitzgerald, B. 1999. "Unpacking the Systems Development Process: An Empirical Application of the Csf Concept in a Research Context," *Journal of Strategic Information Systems* (8:4), pp 351-371.

Calder, A. 2006. *Information Security Based on Iso 27001/Iso 17799: A Management Guide*. Van Haren Publishing.

Calder, A., and Watkins, S. 2008. *It Governance: A Manager's Guide to Data Security and Iso 27001/Iso 27002*. London, UK: Kogan Page Ltd.

Chan, M., Woon , I., and Kankanhalli, A. 2005. "Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior," *Journal of Information Privacy and Security* (1:3), pp 18-41.

Chin, W.W. 1998. "Issues and Opinion on Structural Equation Modeling," *MIS Quarterly* (22:1), pp 7-16.

Cohen, A.R. 1959. *Situational Structure, Self-Esteem, and Threat-Oriented Reactions to Power*. Ann Arbor: Institute for Social Research.

Conger, J.A., and Kanungo, R.N. 1988. "The Empowerment Process: Integrating Theory and Practice," *Academy of Management Review* (13:3), pp 471-482.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp 79-98.

Datta, L. 1982. "Strange Bedfellows: The Politics of Qualitative Methods," *American Behavioral Scientist* (26:1), pp 133-144.

Dehning, B., Richardson, V.J., and Zmud, R.W. 2007. "The Financial Performance Effects of It-Based Supply Chain Management Systems in Manufacturing Firms," *Journal of Operations Management* (25:4), pp 806-824.

Delone, W., and McLean, E. 2003. "The Delone and Mclean Model of Information Systems Success: A Ten-Year Update," *Journal of Management Information Systems* (19:4), pp 9-30.

Dhillon, G. 2007. *Principles of Information Systems Security: Text and Cases*. Hoboken, NJ: Wiley.

Dickinson, R., Ferguson, C., and Sircar, S. 1985. "Setting Priorities with Csfs," *Business Horizons* (35:2), pp 44–47.

Dukes, W. 1965. "N = 1," *Psychological Bulletin* (64:1), pp 74-79.

Ein-Dor, P., and Segev, E. 1978. "Organizational Context and the Success of Management Information Systems," *Management science* (24:10), pp 1064-1077.

Fornell, C., and Larcker, D. 1981. "Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics," *Journal of Marketing Research* (18:3), pp 382-388.

Fyffe, G. 2008. "Addressing the Insider Threat," *Network Security* (2008:3), pp 11-14.

Gatzlaff, K.M., and McCullough, K.A. 2010. "The Effect of Data Breaches on Shareholder Wealth," *Risk Management and Insurance Review* (13:1), pp 61-83.

Guynes, C.S., and Vanecek, M.T. 1996. "Critical Success Factors in Data Management," *Information & Management* (30:4), pp 201-209.

Huberman, A., and Crandall, D. 1982. "Fitting Words to Numbers: Multisite/Multimethod Research in Educational Dissemination," *American Behavioral Scientist* (26:1), pp 62-83.

Kahn, R.L., Wolfe, D.M., Quinn, R.P., Snoek, J.D., and Rosenthal, R.A. 1964. *Organizational Stress: Studies in Role Conflict and Ambiguity*. NY: Wiley.

Kankanhalli, A., Teo, H.H., Tan, B.C.Y., and Wei, K.K. 2003. "An Integrative Study of Information Systems Security Effectiveness," *International Journal of Information Management* (23:2), pp 139-154.

Katz, D., and Kahn, R.L. 1978. *The Social Psychology of Organizations*, (2 ed.). NY: Wiley.

Khansa, L., and Liginlal, D. 2011. "Predicting Stock Market Returns from Malicious Attacks: A Comparative Analysis of Vector Autoregression and Time-Delayed Neural Networks," *Decision Support Systems* (Forthcoming), p 15.

Kidd, C., Orr, R., Abowd, G., Atkeson, C., Essa, I., MacIntyre, B., Mynatt, E., Starner, T., and Newstetter, W. 1999. "The Aware Home: A Living Laboratory for Ubiquitous Computing Research," *Cooperative Buildings. Integrating Information, Organizations and Architecture*), pp 191-198.

Kotulic, A.G. 2001. "The Security of the It Resource and Management Support: Security Risk Management Program Effectiveness." Arlington: The University of Texas at Arlington, p. 225.

Kotulic, A.G., and Clark, J.G. 2004. "Why There Aren't More Information Security Research Studies," *Information & Management* (41:5), pp 597-607.

Lam, W. 2005. "Investigating Success Factors in Enterprise Application Integration: A Case-Driven Analysis," *European Journal of Information Systems* (14:2), pp 175-187.

Lee, A. 1989. "A Scientific Methodology for Mis Case Studies," *MIS Quarterly* (13:1), pp 33-50.

Lee, R.M. 1993. *Doing Research on Sensitive Topics*. Newbury Park, CA: Sage Publications Ltd.

Lee, S.M., Lee , S.G., and Yoo, S. 2004. "An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories," *Information & Management* (41:6), pp 707-718.

Magal, S.R., Carr , H.H., and Watson, H.J. 1988. "Critical Success Factors for Information Center Managers," *MIS Quarterly* (12:3), pp 413-425.

Magklaras, G., and Furnell, S. 2005. "A Preliminary Model of End User Sophistication for Insider Threat Prediction in It Systems," *Computers & Security* (24:5), pp 371-380.

March, J.G., and Shapira, Z. 1987. "Managerial Perspectives on Risk and Risk Taking," *Management Science* (33:11), pp 1404-1418.

Martin, E.W. 1982. "Critical Success Factors of Chief Mis/Dp Executives," *MIS Quarterly* (6:2), pp 1-9.

McGrath, J.E. 1976. "Stress and Behavior in Organizations," *Handbook of industrial and organizational psychology*), pp 1351-1395.

Miles, M.B. 1982. "A Mini-Cross-Site Analysis: Commentary on These Studies," *American Behavioral Scientist* (26:1), pp 121-131.

Mukherjee, I. 2008. "The Complexity Paradigm: Implications for Information Systems and Their Strategic Planning," *Journal of Computer Science* (4:5), pp 382-392.

Nunnally, J.C., and Bernstein, I.H. 1994. *Psychometric Theory*, (3 ed.). NY: McGraw Hill.

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' Behavior Towards Is Security Policy Compliance," *40th Hawaii International Conference on System Sciences*, p. 156b.

Parker, D. 1981. *Computer Security Management*. Reston, VA: Reston Publishing Company.

Paulk, M.C., Curtis, B., Chrissis, M.B., and Weber, C.V. 1993. "Capability Maturity Model, Version 1.1," *IEEE Software* (10:4), pp 18-27.

Peffers, K., Gengler, C., and Tuunanen, T. 2003. "Extending Critical Success Factors Methodology to Facilitate Broadly Participative Information Systems Planning," *Journal of Management Information Systems* (20:1), pp 51-85.

Ponemon. 2010. "2010 Annual Study: U.S. Cost of a Data Breach." Retrieved April 20, 2011, from http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf

Riddell, K. 2011. "Security-Breach Costs Climb 7% to $7.2 Million Per Incident." Retrieved May 10, 2011, from http://www.bloomberg.com/news/print/2011-03-08/security-breach-costs-climb-7-to-7-2-million-per-incident.html

Rockart, J.F. 1979. "Chief Executives Define Their Own Data Needs," *Harvard Business Review* (57:2), pp 81-93.

Sabherwal, R., and Kirs, P. 1994. "The Alignment between Organizational Critical Success Factors and Information Technology Capability in Academic Institutions," *Decision Sciences* (25:2), pp 301-330.

Sarker, S., and Lee, A. 2003. "Using a Case Study to Test the Role of Three Key Social Enablers in Erp Implementation," *Information & Management* (40:8), pp 813-829.

Schmidt, R., Lyytinen, K., Keil, M., and Cule, P. 2001. "Identifying Software Project Risks: An International Delphi Study," *Journal of Management Information Systems* (17:4), pp 5-36.

Schriesheim, C.A., and Eisenbach, R.J. 1995. "An Exploratory and Confirmatory Factor-Analytic Investigation of Item Wording Effects on the Obtained Factor Structures of Survey Questionnaire Measures," *Journal of Management* (21:6), pp 1177-1193.

Sennewald, C.A. 2003. *Effective Security Management*, (4 ed.). Butterworth-Heinemann.

Shenkar, O., and Zeira, Y. 1992. "Role Conflict and Role Ambiguity of Chief Executive Officers in International Joint Ventures," *Journal of International Business Studies* (23:1), pp 55-75.

Siponen, M. 2005. "An Analysis of the Traditional Is Security Approaches: Implications for Research and Practice," *European Journal of Information Systems* (14:3), pp 303-315.

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp 487-502.

Smith, E.E. 1957. "The Effects of Clear and Unclear Role Expectations on Group Productivity and Defensiveness," *Journal of Abnormal and Social Psychology* (55:2), pp 213-217.

Sneha, S., and Varshney, U. 2009. "Enabling Ubiquitous Patient Monitoring: Model, Decision Protocols, Opportunities and Challenges," *Decision Support Systems* (46:3), pp 606-619.

Spears, J.L., and Barki, H. 2010. "User Participation in Information Systems Security Risk Management," *MIS Quarterly* (34:3), pp 503-522.

Stanton, J., Stam, K., Mastrangelo, P., and Jolton, J. 2005. "Analysis of End User Security Behaviors," *Computers & Security* (24:2), pp 124-133.

Stephenson, W. 1953. *The Study of Behavior: Q-Technique and Its Methodology*. University of Chicago Press.

Straub , D.W. 1990. "Effective Is Security," *Information Systems Research* (1:3), pp 255-276.

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

Tannenbaum, A.S., and Cooke, R.A. 1978. "Organizational Control: A Review of Research Employing the Control Graph Method," in: *Organizations Alike and Unlike*, D.J. Hickson (ed.). London: Routledge and Kegan Paul ltd, pp. 183-210.

Tsoumas, B., and Gritzalis, D. 2006. "Towards an Ontology-Based Security Management," *20th International Conference on Advanced Information Networking and Applications*, pp. 985-992.

von Solms, R., van de Haar, H., von Solms, S.H., and Caelli, W.J. 1994. "A Framework for Information Security Evaluation," *Information & Management* (26:3 (March)), pp 143-153.

Wason, K.D., Polonsky, M.J., and Hyman, M.R. 2002. "Designing Vignette Studies in Marketing," *Australasian Marketing Journal* (10:3), pp 41-58.

Weiser, M. 1991. "The Computer for the 21st Century," *Scientific American* (265:3), pp 94-104.

Workman, M., Bommer , W.H., and Straub, D.W. 2008. "Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test," *Computers in Human Behavior* (24:6), pp 2799-2816.

Workman, M., and Gathegi, J. 2007. "Punishment and Ethics Deterrents: A Study of Insider Security Contravention," *Journal of the American Society for Information Science and Technology* (58:2), pp 212-222.

Yin, R. 1994. *Case Study Research: Design and Methods*, (2 ed.). Thousand Oaks: Sage Publications.

Zhuang, Y. 2005. "Does Electronic Business Create Value for Firms? An Organizational Innovation Perspective," *Journal of Electronic Commerce Research* (6:2), pp 146-159.

Appendix A (Questionnaire)

SRM Effectiveness (SRM)

1) Relative to our type of industry, security is very effective at this location.

Not at all						To a large extent
1	2	3	4	5	6	7

2) Our security policy is understood by management.

Not at all						To a large extent
1	2	3	4	5	6	7

3) Our security policy is understood by end users (e.g. staff).

Not at all						To a large extent
1	2	3	4	5	6	7

4) Internal operations that rely on accurate and timely data information have not been negatively impacted by security measures.

Not at all						To a large extent
1	2	3	4	5	6	7

5) We have protective security measures in place that are cost-effective and have reduced the level of risk to acceptable levels.

Not at all						To a large extent
1	2	3	4	5	6	7

Executive Management Support (EMS)

6) Senior management has fully supported the establishment of plans, policies, programs, and guidelines for information security.

Not at all						To a large extent
1	2	3	4	5	6	7

7) The information security function is supported with appropriate resources to perform its function in system design, test, and evaluation.

Not at all						To a large extent
1	2	3	4	5	6	7

8) Senior management takes an active role in development and implementation of security controls.

Not at all						To a large extent
1	2	3	4	5	6	7

Organizational Maturity (OM)

9) The organization has a formal program of roles and responsibilities that are known to everyone.

Not at all						To a large extent
1	2	3	4	5	6	7

10) The current security awareness program effort was in reaction in large part to actual or suspected past instances of security breaches at this location.

Not at all						To a large extent
1	2	3	4	5	6	7

11) We use audit reviews to evaluate the levels of risk in order to identify levels that exceed acceptable limits established by management.

Not at all						To a large extent
1	2	3	4	5	6	7

Open Communication (OC)

12) When a formal security policy initiative is launched, visibility is given to the event through devices such as management presentations and question/answer forums.

Not at all						To a large extent
1	2	3	4	5	6	7

13) Management communicates visibly and seriously regarding the need to protect the confidentiality of sensitive information.

Not at all						To a large extent
1	2	3	4	5	6	7

Risk Management Stakeholders (RMS)

14) The current security policy is the result of inputs from many members of our organization.

Not at all						To a large extent
1	2	3	4	5	6	7

15) Auditors and security personnel are involved in design changes in information systems.

Not at all						To a large extent
1	2	3	4	5	6	7

Team Member Empowerment (TME)

16) Getting authorization to access data that would be useful in my function is time consuming and difficult.

Not at all						To a large extent
1	2	3	4	5	6	7

17) Data that would be useful to my function is unavailable because we do not have the right authorization.

Not at all						To a large extent
1	2	3	4	5	6	7

18) The decentralized organization of the unit's Information Security Services with respect to personnel who carry out security policy related work is beneficial.

Not at all						To a large extent
1	2	3	4	5	6	7

19) The decentralized organization of the unit's Information Security Services with respect to securing hardware and software is beneficial.

Not at all						To a large extent
1	2	3	4	5	6	7

Holistic View of an Organization (HVO)

20) The organization's business objectives and goals include compliance with a broad-level security policy.

Not at all						To a large extent
1	2	3	4	5	6	7

21) There is strong insistence on a uniform managerial style throughout the organization.

Not at all						To a large extent
1	2	3	4	5	6	7

Security Maintenance (SM)

22) The role based access control procedures offered are sufficient.

Not at all						To a large extent
1	2	3	4	5	6	7

23) The organization takes adequate steps in updating the SRM policy.

Not at all						To a large extent
1	2	3	4	5	6	7

Corporate Security Strategy (CSS)

24) The organization provides adequate support for the intellectual property rights issues associated with in-house security solutions (e.g. patent support etc).

Not at all						To a large extent
1	2	3	4	5	6	7

25) The organization supports development of in-house security software.

Not at all						To a large extent
1	2	3	4	5	6	7

Human Resource Development (HRD)

26) The organization offers sufficient security training to members who are directly involved with the security risk management process.

Not at all						To a large extent
1	2	3	4	5	6	7

27) Personnel responsible for executing the security risk management process have sufficient experience to deal with security related incidents.

Not at all						To a large extent
1	2	3	4	5	6	7

Appendix B

Scenario 1 (Executive manager)

Jeffrey accidentally removes a customer's file from the main database. Upon realizing his error he reports the instance to his department head, who is obligated to report it to the VP of Internal Audit. Jeffrey's privileges are taken away until an investigation is carried out and completed.

Scenario 2 (Staff employee)

As a help desk employee, John has certain access to hardware that might allow him to compromise hardware or software. Also, John, due to his ability to purchase technologies below a certain threshold, may unintentionally purchase something that is inherently insecure.