8-6-2011

Critical Success Factors for an Effective Security Risk Management Program: An Exploratory Case Study at a Fortune 500 Firm

Humayun Zafar
Kennesaw State University, hzafar@kennesaw.edu

Jan G. Clark
The University of Texas at San Antonio, jan.clark@utsa.edu

Myung Ko
University of Texas at San Antonio, myung.ko@utsa.edu

Yoris A. Au
The University of Texas at San Antonio, yoris.au@utsa.edu

Critical Success Factors for an Effective Security Risk Management Program: An Exploratory Case Study at a Fortune 500 Firm

Humayun Zafar
Kennesaw State University
hzafar@kennesaw.edu

Jan G. Clark
The University of Texas at San Antonio
jan.clark@utsa.edu

Myung Ko
The University of Texas at San Antonio
myung.ko@utsa.edu

Yoris A. Au
The University of Texas at San Antonio
yoris.au@utsa.edu

ABSTRACT

We investigate differences in perception between management and staff with regard to the influence of critical success factors (CSFs) on security risk management (SRM) effectiveness at a Fortune 500 company. Nine CSFs are confirmed to exist in the organization. Management and staff agree that each CSF is important for SRM effectiveness, but differ on the level of importance of each CSF. With regard to six of the nine CSFs (executive management support, organization maturity, open communication, holistic view of organization, corporate security strategy, and human resource development), management and staff concur on their current implementation, and have a positive perception about their impact. The results also indicate that both management and staff are not satisfied with the current practices pertaining to risk management stakeholders, team member empowerment, and security maintenance. Recommendations are presented for the organization as part of possible solutions to counter the dissatisfaction with these three CSFs.

Keywords

Security risk management, critical success factors, and information security

INTRODUCTION

Information security is a complex, multidimensional issue that can have a great impact on organizations. Understanding potential threats, educating personnel in security awareness, and establishing and executing security policies are a part of an organization's security culture (Dhillon 2007). However, research in this area is still in its infancy. Methods of research in information security have been proposed and compared at length (Siponen 2005), but have not been used to their full extent in organizational level studies. In an organization, security can only be enhanced if there is holistic support for all security risk management (SRM) policies and procedures. We parallel the definition of Blakley et al. (2001) by considering security risk management as a series of mechanisms which have been put in place by an organization to counter or prevent an information security related event.

Straub and Welke (1998) state that organizational systems are less secure than they might be if top managers, middle managers, and employees neglect information security procedures. In this backdrop, it is surprising that none of the studies have concentrated on the link between management and staff in terms of establishing effective SRM policies. Information security policies are not mutually exclusive procedures for an individual department in an organization. Instead, they need to be viewed synergistically across all levels and stakeholders. Management may have varying perspectives of expected SRM strategies than those of the workers. This can result in differences in the actual effectiveness of SRM programs. Studies have shown that issues become more complex when management is unable to view risk from all perspectives (March et al. 1987). To address this disconnect, factors that are critical for an organization to operate an effective SRM should be addressed. Therefore, The purpose of this study was twofold: 1) identify CSFs that may highlight differences in perceptions of SRM effectiveness among management and staff, and 2) ascertain their effects using role theory organization (Kahn et al. 1964) as the baseline theory at a single Fortune 500 firm, heretofore known as The Company.

To our knowledge, this is the first time the CSF method has been used in the context of SRM effectiveness with a theoretical perspective. In fact, organizational level studies that consider SRM in the context of an actual business setting are currently lacking in IS research (Smith et al. 2010).

We intended to answer the following research question: What is the impact of perceived CSFs on the perceived effectiveness of an organization's SRM program? Perceived security effectiveness is defined as the subjective probability with which the management and staff believe that their information (personal or work related) will not be viewed, stored, and manipulated by inappropriate parties in a manner consistent with their expectations based on the current SRM implementation.

We applied the CSF method in an in-depth study of a single organization. Precedence of using the CSF approach in a single organization has been set (Shank et al. 1985; Slevin et al. 1991). Similar to Bullen and Rockart (1981a), we investigated layers of management. However, we went one-step further and included the staff layer as well. To accomplish this task, we identified initial CSFs extracted from role theory based on previous research. This was done to provide theoretical rigor to the study. The initial CSFs were executive management support (Schmidt et al. 2001), organization maturity (Paulk et al. 1993), open communication (Brown et al. 1995), risk management stakeholders (Keil et al. 2002), team member empowerment (Conger et al. 1988), and holistic view of an organization (Lam 2005). To maintain the integrity of the CSF method the initial CSFs were confirmed through interviews with management and staff, and new CSFs were also identified.

LITERATURE REVIEW

In IS, CSFs have been used 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 et al. 1984). CSFs can also be used as an MIS planning tool by interviewing multiple levels of managers in an organization (Bullen et al. 1981b). Other CSF research in the IS discipline includes areas such as the IS development process (Butler et al. 1999), IS planning (Bowman et al. 1983), organizational performance (Raghunathan et al. 1989), performance evaluation (Bergeron et al. 1989), e-commerce (Laosethakul et al. 2006), ERP systems (Soliman et al. 2001), data management (Guynes et al. 1996), e-banking (Shah et al. 2007), and inter-organizational information system (Lu et al. 2006). 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 (Chang et al. 2006).

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 et al. 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.

RESEARCH METHOD

This study employed the CSF method at The Company, with the unit of analysis being the level of an employee (management levels and staff). The Company is a Fortune 500 business that has experienced significant growth. IT security related decisions are centralized and are made by a senior security manager. Their Division Security Program highlights aspects of security such as personnel security, information and systems security, physical security, communications security, and industrial security administrative management for the overall facility. The senior security manager controls all aspects of the organization's security operations, and is assisted by at least one other junior manager. They are responsible for establishing training and development plans, goal setting congruent with the Company's goals, developing the security department's budget, and implementing new and updated security policies. They are also responsible for conducting and assisting with multi-agency security audits and assessing the overall effectiveness of the facilities security processes to ensure full compliance. The Company considers its Division Security Program as a cornerstone for protecting its assets against internal as well as external threats.

There is a strong case-study tradition in the IS field (Benbasat et al. 1987; Kling et al. 1984; Lee 1989; Markus 1983; Sarker et al. 2003). Various researchers have also been attempting to address methodological issues such as lack of control and generalizability that arise when a case study is conducted (Datta 1982; Dukes 1965; Huberman et al. 1982; Miles 1982). To counter these issues, we implemented guidelines that have been presented for the

positivist case research paradigm (Lee 1989; Yin 1994). These guidelines have also been successfully applied (Sarker et al. 2003), which in turn enhance the internal, construct, and external validities of the study. In addition to those recommendations, we also enhanced statistical conclusion validity through homogeneity of subjects (Shadish et al. 2002). Finally we implemented data triangulation through converging lines of inquiry such as observations, questionnaire, and interviews. For organizational level studies, questionnaires are the most suitable form of data collection (Stone 1978). Hypothetical case scenarios preceded the questionnaire. We contend that presenting a respondent with the opportunity of creating a simulated case rather than a direct question about their organization's SRM policies resulted in a more honest gauge of their perceptions regarding the current SRM program at The Company.

RESULTS

The data were collected at one of the major company sites, which contained 513 full time employees. Both qualitative and quantitative results are presented, along with discussion of results.

Qualitative Results

This includes confirmation of initial CSFs, and extraction of new CSFs.

Critical Success Factors

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 of The Company took part in this portion of the study. These employees were randomly selected, and notified in advance about the option of interviewing. The interviews were then scheduled based on each employee's available dates and times.

As part of the CSF confirmation/disconfirmation process, each participant was asked to create hypothetical scenarios related to potential violation of an SRM policy and its impact on The Company. 14 of the 32 interviewees provided scenarios. The use of scenarios as a precursor to the CSF method formed the backbone of some of the discussions with the top two management layers.

The scenarios served as a lead-in to discussion of the initial CSFs. After explaining what each one entailed, participants were asked to assess their applicability to The Company. Based on meetings with each of the 32 employees, the initial CSFs were confirmed. Their scenarios were used to encourage extraction of important factors related to the current SRM program that were not considered as part of the initial CSFs, but in a participant's opinion were important. This formed the basis of the extraction of new CSFs, which are described next.

Extraction of New CSFs

One thing that became clearer as each interview progressed was that there is a difference in opinion between management and staff with regard to what is an important component of an effective SRM program. To some extent, this was witnessed in the type of scenarios that were created by those who were interviewed. Management had a tendency to look at the "big-picture," whereas staff concentrated on the mechanics of security. However, when shown the CSFs of the other group, each group agreed with them. A common statement in those cases was "That's a good way of putting it" or "I never really thought of it that way, but yes it does complement with what we are wanting to achieve."

Senior members of the SRM management team are acutely aware of the challenges The Company faces in developing an SRM program that complies with both U.S. and European regulations. As a global organization, this is considered as one of the critical requirements for The Company. According to one executive, The Company deals 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 deals with "the data protection directive, which unlike U.S. regulations such as HIPPA or Sarbanes-Oxley acts, provides few specifics as to how these privacy requirements should be met." While creating the SRM program, management therefore focuses on the need to establish a consistent set of requirements common to various U.S. and EU jurisdictions, while keeping in mind The Company's own standards for protecting customer and supplier data. This is through enhanced security features such as encryption. This is also why, according to a middle manager, The Company focuses on creating in-house security tools as part of their corporate security strategy. It allows the organization to build a foundation that is both deep and broad, rather than a series of narrow solutions that address regulations on a case-by-case basis.

Overall, staff knows very little about the various U.S. and EU directives. However, most members of staff agree that it is important to encourage growth of corporate security strategies because it makes 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 has its disadvantages. Accordingly, when a division is informed that an assessment will occur, it changes its current practices to what is required as part of the SRM program. However, as soon as the division passes the assessment, the makeshift (required) processes are removed in favor of the initial practices.

Discussions during these interviews resulted in three additional CSFs: security maintenance, corporate security strategy, and human resource development. The interviewed personnel were presented a final list of CSFs, and they were agreed upon by both management and staff. A point to note is that after interviewing 20 candidates, no new information with regard to different CSFs was gathered from the employees. Hence, it was decided that 32 participants for this phase of the study was sufficient.

We incorporated Kotulic's (2001) questionnaire to study the impact of CSFs on SRM effectiveness. However, the questionnaire had to be updated to incorporate the new CSFs. Table 1 summarizes the contents of the questionnaire with regard to each CSF. The complete questionnaire has not been provided due to space limitations.

Concept	Construct	Operationalization
SRM effectiveness	SRM	Statements on perception of how secure the current SRM is, along with it being understood by all stakeholders.
Executive management support	Management	Statements on role of executive management as supporters of the SRM process.
Organizational maturity	Maturity	Statements on existence of formal responsibilities and rules.
Open communication	Communication	Statements on communication levels with regard to the SRM process.
Risk management stakeholders	Stakeholders	Statements on who is involved in the SRM process.
Team member empowerment	Empowerment	Statements on authority on part of employees to make decisions.
Holistic view of an organization	Holistic	Statements on the scope of the SRM policies and its management.
Security maintenance	Maintenance	Statements on scope of security procedures and policy updates.
Corporate security strategy	Strategy	Statements on protection of intellectual property rights and supplementing (in-house) software.
Human resource development	Development	Statements on adequacy of employee experience and training.

Table 1: Questionnaire Contents

The next section describes the steps that were undertaken to check for validity and reliability of the survey instrument that would later be used to check for differences in perception of SRM effectiveness.

Validity and Reliability

A previously validated questionnaire was used to measure the initial CSFs. However, since new CSFs were extracted during the interview process, the questionnaire was updated to include the three additional CSFs. 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 The Company to ascertain if the questions being asked were appropriate for each construct. This assisted in enhancing the construct validity of the questionnaire, as specified by Nunnally and Bernstein (1994). Refinements were made with regard to the language, and the survey was then administered to 135 Company employees to test for reliability and construct validity.

We used confirmatory factor analysis to gauge construct validity (convergent and discriminant) of the questionnaire. The factor loadings were all above the suggested threshold of 0.6 (Chin 1998). In addition, items that measured the

same construct had higher loadings than those measuring other constructs. This suggests acceptable convergent and discriminant validity. To further assess construct validity, we looked at 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 et al. 1981). Also, the square root of the AVE of each construct was greater than the correlation between the construct and other constructs, suggesting adequate discriminant validity.

Reliability was assessed using Cronbach's alpha and composite reliability. The alpha value and composite reliability for each construct was above 0.7, the suggested threshold for adequate reliability (Nunnally et al. 1994). Once the reliability and validity were ascertained, the survey was administered to the rest of the employees. The next section provides the quantitative results for the participants of the study.

Quantitative Results

272 out of 378 employees, excluding those who participated in the pilot study, took part in the survey portion of the study. Hence, the response rate was 71.96%.

The validated survey included interval multiple scaled items representing each of the CSFs. Perception of SRM effectiveness at The Company was also a part of the questionnaire. Employees across all layers of management (executive, middle, and lower) and staff were asked to complete the questionnaire. The independent variables were the nine CSFs along with dummy regressors for management and staff. The dependent variable was SRM effectiveness.

Before running the regression models, the data collected from the surveys was checked for against violation of any of the standard regression assumptions, which included heteroskedasticity. Breusch-Pagan test (1979) was used to gauge its presence. If it was present then we ran a generalized least squares (GLS) regression to correct the residual heteroskedasticity. The tabulated results beginning in Tables 2 and 3 present both OLS and GLS estimates, along with the t-values returned by the Breusch-Pagan test.

All layers of management (executive, middle and lower) were combined into a single layer to determine if there were macro-level differences in perceived SRM effectiveness with regard to the CSFs. This comparison provided an abstract view of which group as a whole (management or staff) considered the CSFs more important than the other.

We first considered the single management layer and staff model without taking into account any interaction effects. For this category, the regression equation was:

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

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

Table 2 presents regression coefficients for each of the CSFs as well as the MGT dummy. The GLS estimates show that when controlling for the two groups, all the CSFs are significant. It is interesting to note the negative coefficients for RMS, TME, and SM. This implies that, at both management and staff levels, risk management stakeholders (RMS), team member empowerment (TME), and security maintenance (SM) had a negative impact on SRM effectiveness. Conversations with some of the management and staff of The Company provided insight on these results. In regard to the negative coefficients for risk management stakeholders and team member empowerment, it was proposed that too many people involved with the SRM process may complicate matters unnecessarily and be detrimental to the process itself. According to a senior staff employee, although decisions can be made by individual divisions, most of these decisions have to be approved by senior management of that division. Considering the number of people involved in the approval process, some decisions have been denied or miscommunicated. The staff member suggested that it would be better to have fewer people involved in the decision approval process.

In regard to security maintenance, repeated patch updates to in-house or off-the-shelf security software may encourage employees to think negatively about the effectiveness of the current SRM program. A staff member mentioned that he and his coworkers were surprised by the number of updates that had been applied to most of their in-house programs. According to this employee, it was difficult to imagine why a custom program would require that many update patches.

	OLS (Adj. R^2: 0.85) *p-value < 0.05		Breusch-Pagan Test Significant?	GLS (Adj. R^2: 0.99) *p-value < 0.05	
Coefficients	Estimate	t-value	Yes. (p-value: 0.0011)	Estimate	t-value
Intercept	0.68	3.55*		0.72	20.32*
EMS	0.42	8.26*		0.40	31.85*
OM	0.10	1.66		0.10	7.50*
OC	0.15	2.46*		0.18	15.14*
RMS	-0.10	-1.80		-0.12	-11.64*
TME	-0.12	-2.78*		-0.13	-18.90*
HVO	0.23	3.70*		0.23	18.30*
SM	-0.06	-0.98		-0.06	-6.29*
CSS	0.10	1.79*		0.09	13.35*
HRD	0.15	3.45*		0.16	30.03*
MGT	-0.40	-3.13*		-0.43	-19.22*

Table 2: Single Management Layer and Staff without Interaction Effects

Looking at GLS estimates individually we see that staff considers EMS, OM, OC, and HVO to be more important with respect to SRM effectiveness than management. Staff also considers RMS, and TME to be a detriment toward SRM effectiveness, but not as much as management. Also according to Table 2, although both management and staff recognize the impact (positive or negative) of how a given CSF impacts SRM effectiveness at The Company, there is a difference between the level of importance each group places on the CSFs.

With regard to the new CSFs we see that staff considers CSS and HRD to be more important contributing factors towards SRM effectiveness than management. However, both management and staff consider SM to have a negative impact on SRM effectiveness. In this case, management considers The Company's security maintenance (SM) to be a greater detriment to SRM effectiveness than staff.

Although Table 2 shows that management and staff had varying views on the level of importance of the CSFs, an incremental *F* test was used to compare the two models and determine if these differences were statistically significant. The null and alternate hypotheses were as follows:

$$H_0 \ : \ \delta_S - \delta_{MGT} = 0$$
$$H_1 \ : \ \delta_S - \delta_{MGT} > 0$$

For the null (constrained) model MGT was '0", and for the alternate (unconstrained) model, MGT was "1." The F statistic was 369.42 ($p < 0.05$). This shows that there is a statistically significant difference between staff and management with respect to SRM effectiveness. Although each group considers each of the CSFs important for SRM effectiveness, they differ in how the CSFs impact the effectiveness. Therefore, the initial explanation of importance paid by each group with respect to the impact of the CSFs on SRM effectiveness holds.

As stated earlier, we also checked for interaction effects. In this model the interactions of all CSFs with the groups were also studied. The regression equation was:

$$\begin{aligned} SRM = {} & \beta_0 + \beta_1 EMS + \beta_2 OM + \beta_3 OC + \beta_4 RMS + \beta_5 TME + \beta_6 HVO + \\ & \beta_7 SM + \beta_8 CSS + \beta_9 HRD + \delta_1 MGT + \chi_1 EMS * MGT + \\ & \chi_2 OM * MGT + \chi_3 OC * MGT + \chi_4 RMS * MGT + \chi_5 TME * MGT + \\ & \chi_6 HVO * MGT + \chi_7 SM * MGT + \chi_8 CSS * MGT + \chi_9 HRD * MGT + \varepsilon \end{aligned} \quad (2)$$

Table 3 shows the GLS estimates for the model presented in equation (2). Not all of the interaction effects were significant. Due to the modeling of interactions effects, regression coefficients for each CSF cannot be interpreted directly. Therefore, the RMS coefficient in this case was (-0.21+ 0.17 = -0.04). This shows that even taking into

consideration interaction effects, employees consider the current RMS practices detrimental to SRM effectiveness. Negative coefficients similar to the non-interaction model were also obtained for both TME and SM. For the other CSFs except open communication (OC), the statistically significant net regression coefficients were positive, indicating a positive impact on SRM effectiveness.

	OLS (Adj. R^2: 0.86) *p-value < 0.05		Breusch-Pagan Test Significant?	GLS (Adj. R^2: 0.99) *p-value < 0.05	
Coefficients	Estimate	t-value	Yes. (p-value: 0.0006)	Estimate	t-value
Intercept	0.64	3.11*		0.58	16.26*
EMS	0.22	3.04*		0.22	24.06*
OM	0.15	2.07*		0.17	10.10*
OC	0.22	2.89*		0.22	11.53*
RMS	-0.17	-2.34*		-0.21	-14.54*
TME	-0.14	-2.33*		-0.13	-8.70*
HVO	0.36	4.67*		0.43	15.70*
SM	-0.06	-0.80		-0.07	-5.86*
CSS	0.10	1.54		0.08	4.43*
HRD	0.19	3.58*		0.19	18.50*
MGT	-0.03	-0.08		0.14	1.52
EMS*MGT	0.42	3.93*		0.40	11.79*
OM*MGT	0.03	0.21		0.05	1.45
OC*MGT	-0.19	-1.50		-0.21	-6.39*
RMS*MGT	0.10	0.87		0.17	4.84*
TME*MGT	-0.02	-0.27		0.001	0.05
HVO*MGT	-0.27	-2.06*		-0.37	-6.99*
SM*MGT	-0.05	-0.40		-0.01	-0.35
CSS*MGT	0.05	0.04		-0.03	-0.89
HRD*MGT	-0.18	-1.78		-0.18	-5.78*

Table 3: Single Management Layer and Staff with Interaction Effects

Table 3 shows that in the case of EMS, OM, OC, and HVO staff considers them to be of greater importance compared to management. The overall results are similar in direction to those presented in Table 2. Similar to Table 2, RMS and TME practices are considered by staff to be less of a negative factor in terms of SRM effectiveness compared to management.

In the case of all results shown so far, staff considers EMS, OM, OC, and HVO practices to be more important than management. Whereas, management considers RMS, TME, and SM to have a more negative impact on SRM effectiveness compared to staff. However, in all cases the slope of each line (representing management and staff) is in the same direction. Thus, although both management and staff agree that these are CSFs, they differ on how important each CSF is. Possible reasons for the difference in levels of importance for the CSFs are provided in the next section.

In the case of the new CSFs, again staff lays more importance on CSS and HRD practices with respect to the current SRM program when compared with management. On the other hand management considers SM to have a greater negative impact on SRM effectiveness compared to staff.

Once again, we compared the constrained and unconstrained models to check if the differences found in the interaction models between staff and management were statistically significant. We found that the *F* statistic was

39.727 ($p < 0.05$). This shows that there are significant differences between management and staff with respect to SRM effectiveness when taking into account interaction effects.

IMPLICATIONS AND RECOMMENDATIONS FOR THE COMPANY

This study shows that The Company's management and staff agree that each of the nine CSFs are important for SRM effectiveness. However, they differ on the level of importance of each CSF. With regard six of the nine CSFs (executive management support, organization maturity, open communication, holistic view of organization, corporate security strategy, and human resource development) management and staff concur on their current implementation, and have a positive perception about their impact on SRM effectiveness. However, as stated, the level of importance that each group places on a given CSF is often significantly different. These two observations are not entirely surprising. As previously stated, The Company is considered a leader in its business area, and has gone to great lengths in establishing and maintaining a comprehensive SRM program. Therefore, one would expect both management and staff to agree on the CSFs for their SRM program.

The results indicate that both management and staff are not satisfied with the current practices pertaining to the following CSFs: risk management stakeholders, team member empowerment, and security maintenance. Each of these CSFs had negative coefficients. And, not only were they negative, there was a significant difference in management and staff perceptions. Management was significantly more negative toward these CSF practices than staff. We focus on these three CSFs, and provide recommendations for The Company to counter the negative perception.

With regard to risk management stakeholders, management and staff are concerned about the possibility of insider threats. We suggest that management include privileged identities within the broader Identity Management project scope. This is important because if privileged access is not included in the initial scope, it will not be addressed. The Company should also identify key systems and applications. Current applications in the organization have underlying generic identities, which, once accessed through a privileged account provide wide ranging access to other company applications. The Company should also monitor and report actual adherence to the set policies. It is not sufficient to simply know who is accessing privileged accounts. Account activity should be monitored once access is granted to ensure that the activity itself is compliant with the organization's security and business policies.

Team management empowerment is ostensibly linked to risk management stakeholders. Staff expressed concerns that they were not involved with the SRM process. We suggest that management consider expanding the role of staff. Staff employees prefer suggestion boxes, and other employer based mechanisms that will give then 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.

Security maintenance is the final CSF that is of major concern to management and staff. Currently, The Company relies on a cadre of in-house software engineers who have 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 The Company's own software developers having knowledge about them has diminished. This does not imply that The Company 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 The Company'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 have not been updated. Other than ensuring timely updates, to truly gauge if security bulletins are relevant, we suggest that The Company 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.

CONTRIBUTION AND CONCLUSION

Six initial CSFs (executive management support, organization maturity, open communication, risk management stakeholders, team member empowerment, and holistic view of organization) were extracted from role theory, and

then confirmed as part of the CSF method. New CSFs (security maintenance, corporate security strategy, and human resource development) were also found. The new CSFs dealt with implementation of security policies at The Company. For example, security maintenance revolved around mechanisms for updating existing policies, and role based access controls. Corporate security strategy focused on set-methods of implementing and encouraging in-house security software development. Finally, human resource development presented a criterion for employees who were part of the SRM implementation. Each one of these CSFs had an underlying theme; a congruence of SRM program objectives and policies that would make them effective. This parallels the definition of role compliance.

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

The use of a widely recognized theory from organizational studies in a case study environment allowed greater focus on the role levels of management and staff play with regard to SRM effectiveness. To validate the findings a combination of qualitative and quantitative methods were used. In this study, the impact of roles was quantified through multiple regression models with and without interaction effects.

In summary, this study examined the differences between perceptions between management and staff with regard to SRM effectiveness. Overall, we found significant differences between groups based on macro-level data analysis using a variety of multiple regression models. This exploratory work has set the stage for future research in the area of organizational information security, which can potentially focus on development of theory based hypotheses revolving around the constructs found in this study.

REFERENCES

1. Benbasat, I., Goldstein, D.K., and Mead, M. (1987) The case research strategy in studies of information systems, *MIS Quarterly* 11, 3, pp 369-386.
2. 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.
3. Blakley, B., McDermott, E., and Geer, D. (2001) Information security is information risk management, Workshop on New Security Paradigms, ACM New York, NY, USA, Cloudcrodt, New Mexico, pp. 97-104.
4. Bowman, B., Davis, G., and Wetherbe, J. (1983) Three stage model of MIS planning, *Information & Management* 6, 1, pp 11-25.
5. Boynton, A., and Zmud, R. (1984) An assessment of critical success factors, *Sloan Management Review (pre-1986)* 25, 4, pp 17-27.
6. 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.
7. Brown, S.L., and Eisenhardt, K.M. (1995) Product development: past research, present findings, and future directions, *Academy of Management Review* 20, 2, pp 343-378.
8. Bullen, C., and Rockart, J. (1981a) A primer on critical success factors, *Center for Information Systems Research* Working Paper No. 69, Sloan School of Management, pp 1-64.
9. Bullen, C.V., and Rockart, J.F. (1981b) A primer on critical success factors, *Center for Information Systems Research* Working Paper No. 69, Sloan School of Management, pp 1-64.
10. 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.
11. Chang, S.E., and Ho, C.B. (2006) Organizational factors to the effectiveness of implementing information security management, *Industrial Management & Data Systems* 106, 3, pp 345-361.
12. Chin, W.W. (1998) Issues and opinion on structural equation modeling, *MIS Quarterly* 22, 1, pp 7-16.
13. Conger, J.A., and Kanungo, R.N. (1988) The empowerment process: Integrating theory and practice, *Academy of Management Review* 13, 3, pp 471-482.
14. Datta, L. (1982) Strange bedfellows: The politics of qualitative methods, *American Behavioral Scientist* 26, 1, pp 133-144.
15. Dhillon, G. (2007) *Principles of information systems security: text and cases* Wiley, Hoboken, NJ, p. 450.

16. Dukes, W. (1965) N = 1, *Psychological Bulletin* 64, 1, pp 74-79.
17. 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.
18. Guynes, C.S., and Vanecek, M.T. (1996) Critical success factors in data management, *Information & Management* 30, 4, pp 201-209.
19. Huberman, A., and Crandall, D. (1982) Fitting words to numbers: multisite/multimethod research in educational dissemination, *American Behavioral Scientist* 26, 1, pp 62-83.
20. Kahn, R.L.*, et al.* (1964) *Organizational stress: Studies in role conflict and ambiguity* Wiley, NY.
21. Katz, D., and Kahn, R.L. (1978) *The Social Psychology of Organizations*, (2 ed.) Wiley, NY.
22. Keil, M., Tiwana, A., and Bush, A. (2002) Reconciling user and project manager perceptions of IT project risk: A Delphi study, *Information Systems Journal* 12, 2, pp 103-119.
23. Kling, R., and Iacono, S. (1984) The control of information systems developments after implementation, *Communications of the ACM* 27, 12, pp 1218-1226.
24. Kotulic, A.G. (2001) The security of the IT resource and management support: Security risk management program effectiveness, The University of Texas at Arlington, Arlington, p. 225.
25. Lam, W. (2005) Investigating success factors in enterprise application integration: a case-driven analysis, *European Journal of Information Systems* 14, 2, pp 175-187.
26. Laosethakul, K., Oswald, S., and Boulton, W. (2006) Critical Success Factors for E-Commerce in Thailand: A Multiple Case Study Analysis, AMCIS 2006 Proceedings, pp. 3511-3521.
27. Lee, A. (1989) A scientific methodology for MIS case studies, *MIS Quarterly* 13, 1, pp 33-50.
28. Lu, X.H., Huang, L.H., and Heng, M.S.H. (2006) Critical success factors of inter-organizational information systems--A case study of Cisco and Xiao Tong in China, *Information & Management* 43, 3, pp 395-408.
29. March, J.G., and Shapira, Z. (1987) Managerial perspectives on risk and risk taking, *Management Science* 33, 11, pp 1404-1418.
30. Markus, M.L. (1983) Power, politics, and MIS implementation, *Communications of the ACM* 26, 6, pp 430-444.
31. Miles, M.B. (1982) A Mini-Cross-Site Analysis: Commentary on These Studies, *American Behavioral Scientist* 26, 1, pp 121-131.
32. Nunnally, J.C., and Bernstein, I.H. (1994) *Psychometric theory*, (3 ed.) McGraw Hill, NY.
33. Paulk, M.C.*, et al.* (1993) Capability maturity model, version 1.1, *IEEE Software* 10, 4, pp 18-27.
34. Raghunathan, T., Gupta, Y.P., and Sundararaghavan, P. (1989) Assessing the impact of IS executives' critical success factors on the performance of IS organizations* 1, *Information & Management* 17, 3, pp 157-168.
35. Rockart, J.F. (1979) Chief executives define their own data needs, *Harvard Business Review* 57, 2, pp 81 93.
36. 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.
37. Schmidt, R.*, et al.* (2001) Identifying software project risks: An international Delphi study, *Journal of Management Information Systems* 17, 4, pp 5-36.
38. Shadish, W.R., Cook, T.D., and Campbell, D.T. (2002) *Experimental and quasi-experimental designs for generalized causal inference*, (2 ed.) Wadsworth Publishing, Chicago, IL.
39. Shah, M.H., Braganza, A., and Morabito, V. (2007) A survey of critical success factors in e-Banking: an organisational perspective, *European Journal of Information Systems* 16, 4, pp 511-524.
40. Shank, M.E., Boynton, A.C., and Zmud, R.W. (1985) Critical success factor analysis as a methodology for MIS planning, *MIS Quarterly* 9, 2, pp 121-129.

41. 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.

42. Slevin, D.P., Stieman, P., and Boone, L. (1991) Critical success factor analysis for information systems performance measurement and enhancement. A case study in the university environment, *Information & Management* 21, 3, pp 161-174.

43. Smith, S.*, et al.* (2010) Circuits of Power: A Study of Mandated Compliance to an Information Systems Security De Jure Standard in a Government Organization, *MIS Quarterly* 34, 3, pp 463-486.

44. Soliman, F., Clegg, S., and Tantoush, T. (2001) Critical success factors for integration of CAD/CAM systems with ERP systems, *International Journal of Operations & Production Management* 21, 5/6, pp 609-629.

45. Stone, E.F. (1978) *Research methods in organizational behavior* Goodyear Publishing Company.

46. 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.

47. Yin, R. (1994) *Case study research: Design and methods*, (2 ed.) Sage Publications, Thousand Oaks.