Communications of the Association for Information Systems

Volume 34 Article 37

1-2014

Security Risk Management in Healthcare: A Case Study

Humayun Zafar
Kennesaw State University, hzafar@kennesaw.edu

Myung S. Ko
The University of Texas at San Antonio

Jan G. Clark
The University of Texas at San Antonio

Recommended Citation
Zafar, Humayun; Ko, Myung S.; and Clark, Jan G. (2014) "Security Risk Management in Healthcare: A Case Study," *Communications of the Association for Information Systems*: Vol. 34 , Article 37.
DOI: 10.17705/1CAIS.03437
Available at: https://aisel.aisnet.org/cais/vol34/iss1/37

Communications of the Association for Information Systems

CAIS

Security Risk Management in Healthcare: A Case Study

Humayun Zafar, Ph.D.
Department of Information Systems
Kennesaw State University
hzafar@kennesaw.edu

Myung S. Ko, Ph.D.
The University of Texas at San Antonio

Jan G. Clark, Ph.D.
The University of Texas at San Antonio

Abstract:

We investigated the effectiveness of a security risk management (SRM) program at a large healthcare institution. Using a survey, we explored how nine critical success factors (CSFs): executive management support (EMS), organizational maturity (OM), open communication (OC), risk management stakeholders (RMS), team member empowerment (TME), holistic view for an organization (HVO), security maintenance (SM), corporate security strategy (CSS), and human resource development (HRD) impacted SRM effectiveness. Implementing a mixed research method, we found that employees had a positive perception of SRM toward all CSFs but one—team member empowerment (TME). Both medical professionals and staff had a negative perception of how TME was implemented at the institution.

Keywords: security risk management, healthcare IT, IT security, perceived security.

Editor's Note: The article was handled by the Department Editor for Information Systems and Healthcare.

Volume 34, Article 37, pp. 737-750, January 2014

I. INTRODUCTION

Effective security risk management (SRM) programs in organizations can help balance operational necessities and economic costs associated with information technology (IT)-based systems. SRM is a series of mechanisms that have been put in place by an organization to counter or prevent an information security-related event [Blakley, McDermott, and Geer, 2001]. Some of these mechanisms entail risk assessments, information security policies, and secure computing practice in an organization [Spears and Barki, 2010].

The overall objective of SRM is to enable an organization to adequately handle information. According to Dhillon [2007], SRM is not a standalone activity; it should be integrated with all processes of an organization. This could include understanding potential threats, educating personnel in security awareness, and establishing and executing security policies. Since a SRM program is an enterprise-level implementation with multiple stakeholders (employees, contractors etc.), it is imperative for organizations to establish effective SRM policies and practices. Since employees are the users who interact with information systems on a regular basis in their business activities, the way they use the systems and whether they follow the established guidelines can ultimately influence the overall security of the organization. Considering the overarching impact, it is surprising that organizational-level studies that consider SRM in the context of healthcare industry are currently lacking in IS research. Security risk is inherent in the delivery of healthcare, and it continues to increase due to a rise in direct (network) and indirect (media) connectivity.

The purpose of this study is to explore a SRM program in-depth at the organization level by addressing the research question: What is the perceived effectiveness of an existing security risk management program at a large healthcare institution? Since employees at different job positions may have various beliefs regarding the effectiveness of an organization's SRM policies, exploring these differences in perception increases our understanding of SRM effectiveness. Using a mixed research method approach, a combination of unstructured interviews and an existing SRM-based survey used in a previous study [Zafar, 2011], our study provides a richer understanding of employees' perceptions toward the current SRM program at their healthcare organization. We believe this study is the first that explores SRM effectiveness in the context of the healthcare industry, thereby extending the body of knowledge on this topic.

The remainder of this article is organized as follows. First, we provide a literature review of healthcare IT security and critical success factors (CSFs). Next, we describe our mixed-method research design. This is followed by the results from both quantitative and qualitative analyses. Then, we discuss limitations, implications, and suggestions for future research, and finally, we conclude the article.

II. LITERATURE REVIEW

We looked at two previous research areas relevant to this study: Information security in healthcare and critical success factors. Due to a relative paucity of healthcare research in IS, we looked at some non-IS avenues as well. We used keywords for our search that were a blend of specific and general, such as "healthcare information security," "IT security," "healthcare security," "healthcare IT," "ubiquitous healthcare," "healthcare IT breaches," and "HIPAA breaches."

Information Security in Healthcare

Prior researchers have equated security as being a technical, socio-philosophical [Ratnasingham, 1998] and/or a socio-organizational concern [Dhillon and Backhouse, 2001]. Such demarcation possibly has led to a situation in which security is widely regarded as a field that lacks comprehensive research in information systems [Kotulic and Clark, 2004; Paulson, 2002]. There is a body of work pertaining to generic healthcare IT security. For example, some researchers have focused on keeping information private, as regulated by legislations such as the Health Insurance Portability and Accountability Act [HIPAA, 1996], the Privacy Act of 1974 [FPA, 2007], the Health Information Technology for Economic and Clinical Health (HITECH) Act [Blumenthal, 2010], and the American Recovery and Reinvestment Act (ARRA) [Grumbach and Mold, 2009]. Rindfleisch [1997] found that continued development of enterprise-wide IT systems in healthcare was a doubled-edged sword. On one hand, it was an essential development, since it provided for optimal healthcare. However, it would also inevitably lead to security threats such as intentional and unintentional healthcare information disclosure from insiders, as well as external intruders. Some have argued that legislations such as HIPAA have, in fact, created more security risks [Mercuri,

2004], while others have linked the importance of risk assessments to successful implementation of healthcare IT policies [Eloff and Eloff, 2005; Jepsen, 2003; Matuleviius, Mayer, Mouratidis, Dubois, et al., 2008].

Healthcare IT security research also has focused predominantly on the technical aspects of healthcare IT system implementation [Dwivedi, Bali, Belsis, Naguib, et al., 2003; Epstein, Pasieka, Lord, Wong, et al., 1998; Hu and Weaver, 2004; Kardas and Tunali, 2006; Ng, Sim, and Tan, 2006]. Some work also has been done in the area of maintenance of healthcare IT systems for security reasons. However, since healthcare IT is a relatively new area, most of the concerns regarding the maintenance of technologies to achieve enhanced security have been expressed in terms of updating healthcare security standards of applications [Kokolakis and Lambrinoudakis, 2005], employing new hardware and software techniques [Giakoumaki, Perakis, Tagaris, and Koutsouris, 2008], and developing new platforms for healthcare IT in general [Shoniregun, Dube, and Mtenzi, 2010; Su and Al-Hakim, 2010].

Healthcare IT security research also has looked at media sanitization. Media sanitization deals with disposal, clearing, purging, and destruction of hardware and software that contains critical data [McCallister, Glance, and Scarfone, 2010]. The sanitization procedures may be more complex, depending on factors such as risk to confidentiality and future plans for the media. Once sanitized, it is possible that hardware and software may be sold, given away, or discarded as provided by applicable law or regulation [McCallister et al., 2010].

Researchers also only recently have begun to focus on the requirements for disposing of healthcare IT-related products in a secure manner [Farzandipour, Sadoughi, Ahmadi, and Karimi, 2010; Page, 2010; Park, Seo, Son, Lee, et al., 2010; Smith, 2010]. This research has focused mostly on the overall nature of secure disposal of hardware and software.

In the area of security policies, Gaunt [1998] investigated information security policy in the healthcare field and found the importance of the human element, especially attitude and behavior of staff and their training needs. The author stressed that user participation in the planning and implementation of security is important in promoting organizational security culture. Renaud and Goucher [2012] attempted to understand how information security policies impact health service employees. The authors made some suggestions to address employees' motivational needs by implementing a reward system, facilitating communication and a secure organizational culture, and ensuring fairness in procedures. Using grounded theory, Adams and Blandford [2005] investigated how the different approaches to security and privacy changed users' perceptions in two hospitals. In one hospital, user involvement in the development of application improved corporate awareness across the organization. In another hospital, poor communication from IT regarding security mechanisms was perceived by clinicians as a socially controlling force.

Critical Success Factors (CSFs)

Critical success factors (CSF) are "things" that must go well to ensure success for a manager or an organization [Rockart, 1979]. Zafar [2011] identified nine critical success factors (CSFs) for the perceived effectiveness of a SRM program. They are executive management support (EMS), organizational maturity (OM), open communication (OC), risk management stakeholders (RMS), team member empowerment (TME), holistic view for an organization (HVO), security maintenance (SM), corporate security strategy (CSS), and human resource development (HRD). Each of the CSFs in this framework is discussed next.

Executive management support (EMS) refers to the role of top management in supporting the current SRM program. Several researchers found that top management support is the most important factor for success or in preventing project failures [Jarvenpaa and Ives, 1991; Martin, 1982; Schmidt, Lyytinen, Keil, and Cule, 2001]. If SRM is led from the top, organizations are better able to articulate security in terms of business value. Organizational maturity (OM) deals with existence of formal responsibilities and rules. Mature organizations are those in which systems are formalized and quantified and produce data appropriate to their decision and control processes [Ein-Dor and Segev, 1978; Magal, Carr, and Watson, 1988; Martin, 1982]. Without this maturity, organizations may face significant difficulties in establishing and maintaining an effective SRM program. Open communication (OC) is defined as a free-flow of information within the SRM team and the stakeholders; it will not only reduce the risk of misunderstanding but also ensure that all the relevant stakeholders can contribute as a team. Its relation to an organization's success is considerable [DeLone and McLean, 2003]. Risk management stakeholders (RMS) focuses on engaging a broad base of people because it can elaborate what is important to an organization [Peffers, Gengler, and Tuunanen, 2003]. In the case of an SRM implementation, the stakeholders include all management and staff since they have vested interests in the results of the SRM process and they are integral to the success of an organization's IT ventures. Team member empowerment (TME) refers to the decision-making authority of employees; it has been explored in previous research [Al-Mashari and Zairi, 1999; Sigler and Pearson, 2000]. Most TME research has focused on centralized and decentralized decision structures. Their impact is varied based on factors such as type of organization and size of an organization. Holistic View for an Organization (HVO) pertains to the overall scope of the organization's SRM policies and its management. A more holistic view of an organization

serves as an engine of success of an organization's ventures and also serves as a CSF for organization-wide projects [Lam, 2005]. Security maintenance (SM) is defined as a set of controls and best practices that organizations should adopt to maintain a sufficient security standard [Dhillon, 2007]. Corporate security strategy (CSS) looks at a series of steps undertaken by management to either incorporate security needs or protect intellectual property rights. Finally, human resource development (HRD) refers to education and security training for employees [Dhillon, 2007].

Based on the above, we argue that employees' understanding of these CSFs as they relate to SRM can maximize the overall effectiveness of an organizational SRM program. Thus, we will incorporate the nine CSFs in our analysis to investigate our research question.

III. RESEARCH AND STATISTICAL METHOD

We conducted a survey to assess perceived effectiveness of an SRM program at a major healthcare institution. This survey was part of a prior SRM-based study focused on a single Fortune 500 firm, with a future research recommendation that it could be applied to different organizations in different domains to ascertain external validity. In that study, nine critical success factors (CSFs) for the perceived effectiveness of a SRM program were identified [Zafar, 2011]. Zafar's study adequately implemented guidelines that have been presented for the positivist case research paradigm [Lee, 1989; Yin, 1994]. These guidelines have also been successfully applied [Sarker and Lee, 2003]. Since the survey items have been validated by Zafar [2011], there was no need for revalidation of the survey. Appendix A presents the survey questions, and Appendix B highlights the interview protocol. Perceived SRM effectiveness, which is self-reported by each participant and which deals with how secure the current SRM implementation is, along with nine CSFs, were included in the survey questions.

We carried out onsite unstructured interviews and administered an electronic survey at a large healthcare institution (heretofore referred to as the Agency) in the Southeast United States. The Agency is considered one of the largest providers of healthcare in the United States. It was selected on the basis of its ability to represent most of what healthcare entails (e.g., patient care, use of IT, and a SRM program). We focused on only full-time employees who were either medical professionals (Ph.D.s, MDs, NPs, or RNs), or staff (mostly administrative) because we want to ensure that a more accurate picture of the current state of the SRM program was attained, since all full-time employees have gone through a mandatory HIPAA training. The survey was strictly voluntary. However, an email requesting participation was sent from an internal research department to all full-time employees. Some employees have received additional training through the Agency's extensive crisis coordinator program.

The use of a mixed research model (qualitative and quantitative research techniques) allowed us to provide a richer understanding in an area that to our knowledge has not been investigated in the past. This is especially relevant since certain results may not be explained through numbers alone.

We used generalized least squares regression (GLS) to ascertain the perceived effectiveness of the SRM program at the Agency, which was the dependent variable and the nine CSFs were the independent variables. A dummy regressor was used for medical professionals (MP) and staff.

Data were analyzed using two GLS models. In the first model (Equation 1), macro-level differences in perceived SRM effectiveness were determined. This comparison provided an abstract view of which group as a whole (MPs or staff) considered the CSFs more important than the other. The first model also did not take into account any interaction effects. The GLS equation thus was:

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

In (1), the dummy value MP was "1" if an employee was a medical professional, and "0" otherwise (staff).

The second GLS model took into account interaction effects. In this model, the interactions of all CSFs with the groups were studied. The regression equation was:

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

IV. RESULTS

This section is divided into two subsections: quantitative results and results of our unstructured interviews.

Quantitative Results

In order to gauge differences of perceptions on the SRM effectiveness between medical professionals and staff, we administered a multi-item questionnaire, based on the synthesized list of CSFs. At the time the survey was administered, the Agency had 1521 full-time employees. Overall, 1002 employees participated in the survey. Forty-one records had to be discarded due to reasons such as incomplete information. Therefore, the total number of valid participants was 961 (response rate of 63.2 percent). We believe that the email request by the research department of the Agency was the contributing factor for this high response rate. Table 1 provides a snapshot of those who participated in the survey.

Table 1: Survey Participants

Gender/position	MPs	Staff	Total
Males	162	358	520
Females	87	354	441
Total	249	712	961

Table 2 presents GLS estimates for the model presented in equation (1) and shows regression coefficients for each of the CSFs as well as the MP dummy.

Table 2: MP and Staff—Without Interaction Effects

	GLS (Adj. R^2: 0.72) *p-value < 0.05	
Coefficients	Estimate	t-value
Intercept	0.87	10.12*
EMS	0.80	9.61*
OM	0.22	3.48*
OC	0.20	5.86*
RMS	0.09	5.21*
TME	-0.11	-9.11*
HVO	0.31	8.51*
SM	0.19	9.11*
CSS	0.10	3.99*
HRD	0.21	10.09*
MP	0.14	7.65*

Looking at the GLS estimates individually, we see that EMS has the highest coefficient, followed by HVO. In addition, the MPs had a greater positive perception of the current SRM program (a positive coefficient of MP) compared to staff in regard to EMS, OM, OC, RMS, HVO, SM, CSS, and HRD, since each of these CSFs indicates a significant positive value. This implies that employees are satisfied with how these CSFs are implemented. For example, a positive coefficient and a significant t value for OC imply that the employees are satisfied with the level of communication that in turn facilitates the SRM at the Agency. However, it is interesting to note the negative perception of TME in the eyes of both MPs and staff. Details on the possible reasons for this are provided in the next section (Qualitative Results).

Table 3 presents GLS estimates for the model presented in Equation 2. Due to the modeling of interaction effects, please note that regression coefficients for each CSF cannot be interpreted directly. For example, the EMS coefficient in this case is 0.33 (0.19 + 0.14).

Table 3: MP and Staff—With Interaction Effects		
	GLS (Adj. R^2: 0.71) *p-value < 0.05	
Coefficients	Estimate	t-value
Intercept	0.10	7.12*
EMS	0.19	19.51*
OM	0.19	9.61*
OC	0.13	8.22*
RMS	0.19	3.84*
TME	-0.21	-6.21*
HVO	0.51	5.89*
SM	0.17	2.99*
CSS	0.10	3.13*
HRD	0.19	7.20*
MP	0.11	2.98*
EMS×MP	0.14	9.69*
OM×MP	0.13	4.11*
OC×MP	0.13	3.09*
RMS×MP	0.22	3.13*
TME×MP	-0.10	-3.19*
HVO×MP	0.37	3.28*
SM×MP	0.19	4.19*
CSS×MP	0.10	3.70*
HRD×MP	0.10	3.10*

The coefficients presented in Table 3 also reflect results similar to Table 2. For example, even when taking into account interaction effects, medical professionals (MP) had a positive perception of SRM effectiveness on all CSFs except for TME, since the coefficient on MP is positive and all CSFs but TME indicated positive coefficients and significant t values in Table 3.

Qualitative Results

Unstructured interviews were carried out with employees in various units of the Agency. These interviews occurred after completion of the surveys. Five employees (four men and one woman) from the information security division participated in the interviews. We were also able to interview three more employees (two MPs and one administrative assistant). The purpose was to get their perspective on not only our preliminary results, but also to get their insights on the current SRM process at the Agency. One of the common themes in our conversation with the security division's employees was that the Agency focused heavily on how device manufacturers need to manage security risks pertaining to healthcare systems. The division carries out detailed security risk assessments in the context of security risk management on a quarterly basis. The prime IT security risks, according to them, were risks to data and systems. Also, as a healthcare institution, the Agency has to integrate IT security risk management and patient safety risk management. These two issues are closely intertwined in the area of ubiquitous healthcare.

The employees also discussed how ubiquitous healthcare entails a paradigm shift in healthcare practice, delivery, and view. It focuses on patient-centric operational models promoting real-time monitoring of patients' medical progress, compliance to physicians' advice (such as taking prescription drugs as and when required), and prompt detection of anomalies without time and location dependencies. The fundamental process of ubiquitous healthcare involves the sensing of patient specific information (vital signs, drug compliance, etc.), analysis of collected information for detection of anomalies, and communication of pertinent information to healthcare stakeholders (doctors/nurses/relevant family members) as required. According to them, use of ubiquitous devices can lead to potential IT security-related issues.

Security risk management at the Agency includes scoring of risks, proposing and implementing mitigations for vulnerabilities, summarization of residual risks, collecting security related requirements for the assets, and listing the information assets that need to be protected and understanding their intended use.

Risk assessments include the ability of the Agency's departments to mitigate and have operational workarounds for scenarios such as discontinuity of typical IT services (e.g., network addressing and user authentication) of critical

laboratories on site. Other scenarios include natural disasters, malicious attack on the IT infrastructure, and insider threats.

When we presented the results of our survey and alluded to the negative perceptions of the employees in regard to TME, the interviewees were not surprised. According to them, there is limited authority on the part of a regular medical professional or a staff employee outside their division. Though the Agency has developed a process where any employee may route a new vulnerability to the security division, overall, all security-related matters are the exclusive authority of the division. According to one employee, this ensures centralization of decisions that may impact records management. The employee further stated that "[v]ital records management is an essential tool in our arsenal. We have a records manager who plays a crucial role in the identification, inventory, protection, storage, and accessibility of vital records that support essential functions." This, according to the employees, may be the reason why anyone outside the division may have a negative perception of Team Member Empowerment (TME). According to another security employee, the security office is trying to remove the negative perception. The employee stated that "[w]e are planning to establish a Cyber Security Working Group to share best practices and better prepare and plan for performance of essential functions during potential disruptions." The working group would include a sampling of employees across all the Agency's units, including external partners, such as suppliers and vendors. As far as the other eight factors go, they are a part of a massive security awareness program that the security division sponsors. Also, all employees are required to go through Agency-specific IT security-related training every two years. An employee told us that in "60% of the training sessions, [the] focus is on phishing and internal threats faced. We provide them with hypothetical scenario and try to educate them accordingly." This is in addition to any guidelines laid down by the state and the federal governments.

The interesting thing about the negative perception of TME was that the medical professionals and staff still supported the current status quo. One of the two medical professionals mentioned that, "[a]s an ICU unit chief, I need to make split-second decisions for numerous patients, which impacts them and their families. I do not have time to worry about IT security. There are people here who deal with that." Another MP noted, "[i]n the ER the last thing on my mind is IT security. My attending will judge my medical skills. Paperwork outside of that is not on my mind." Similarly, an administrative assistant reflected, "[o]ur doctors have enough paperwork work to deal with. For them it is better to delegate nonmedical related decisions such as IT security." Based on our observations, the MPs considered delegation as a routine matter, with the assumption that the delegated authority had the capacity to accomplish the task. Although medical professionals have their concern for patients and motivations to complete their task efficiently and effectively, it is important to note that their personal motivations might conflict with overall organizational information security—as indicated by some medical professionals, that IT security is viewed as a nonmedical issue.

V. LIMITATIONS, IMPLICATIONS, AND SUGGESTIONS FOR FURTHER RESEARCH

This study is not without its potential weaknesses. While this case study research provided rich data from both quantitative and qualitative aspects, the findings of the single case study limits the generalizability of results. Future research is needed to assess the generalizability of our findings by replicating our study in different organizational settings. Another limitation of the study is the sample size of the interviews. Compared to survey data that we collected for the quantitative section of our research, we could collect a total of only eight interviews for the qualitative part. However, these interviewees, MPs (attending physicians and residents) (PGY2 or PGY3 Internal Medicine, or PGY2, PGY3, or PGY4 Combined Med-Peds), PGY1 residents (Internal Medicine, Combined Med-Peds, or Transitional Year) understandably lead a very busy work schedule. As researchers we wanted to make sure that we did not take our access for granted or hinder their work in any way. Even with limited interviews, we believe we were able to get valuable insights of people of different backgrounds at the Agency.

This research contributes to the extant literature on SRM by providing additional insights on employees' perceptions toward the SRM program. In addition, this study offers a richer understanding of this research topic in the context of a healthcare organization.

This research also has some practical implications for managers. This study presents an overview of how employees in the same organization with similar training can have opposing points of view pertaining to perceptions of a SRM implementation. Thus, this study raises some concerns whether the SRM training at the Agency is effective, and whether it might be necessary to take some steps to measure employees' understanding of security issues and policies after the training event, perhaps using quizzes or surveys. Previous studies also suggested that we should focus less on formal procedures but focus more on employees when implementing SRM [Lacey, 2010]. Communicating with their employees using newsletters, emails, blogs, and posters could be also effective means to educate employees.

When it comes to healthcare IT security issues in general, the inherent security threats and risks associated with healthcare are yet to be fully resolved, despite the known benefits of ubiquitous computing. These were mentioned in the interview sessions. The enhanced functionalities afforded by the enabling technologies brings increased challenges with respect to data storage, distribution, connectivity, computational power, and energy budgets [Liu, Clark, and Stepney, 2005]. Dealing ethically with critical patient information derived from biometric sensors and mobile devices require systems not only to be reliable and scalable but also to maintain the confidentiality, integrity, and privacy of sensitive health data. Cisco, in its 2010 annual report, predicted that attackers increasingly would target mobile devices as they make their way onto enterprise networks [Cisco, 2011]. This prediction was not too dissimilar from earlier ones [Leavitt, 2005]. The reason the landscape did not change appreciably before was that mobile devices were not attractive and/or lucrative targets for attackers, due to the heterogeneous nature of the technologies involved. Malware development for a single platform did not result in a high number of victims, and altering malware for use on multiple platforms was not as cost effective. However, as mobile devices become homogenous in terms of operating system usage and the backbone networking technologies [Ahmed, Jamal, Mehboob, Khan, et al., 2010], with popular and full-featured SDK APIs, creation of malware will become comparatively trivial, thereby leading to information security concerns. Besides, it is to be noted that wireless communication channels suffer from spotty coverage and are not 100 percent reliable [Sneha and Varshney, 2009]. The sole reliance of ubiquitous healthcare information systems on wireless channels for data communication/ transfer provides further opportunities to malicious agents [Liu et al., 2005].

VI. CONCLUSION

In this study, we explored the perceived effectiveness of a security risk management (SRM) program at a healthcare organization. To our knowledge, this is the first study that used a mixed research case-based approach addressing the SRM aspect in the healthcare industry.

Although SRM programs are implemented to maintain information security in an organization, unless employees at all levels are committed and aware of the SRM policies, the SRM program may not be as effective as it should be, especially for the healthcare organization where risk is inherent in delivering such healthcare.

Our study provides valuable insights on how employees perceive their current SRM program at the organization. Using nine CSFs—executive management support (EMS), organizational maturity (OM), open communication (OC), risk management stakeholders (RMS), team member empowerment (TME), holistic view for an organization (HVO), security maintenance (SM), corporate security strategy (CSS), and human resource development (HRD), we were able to gauge the effectiveness of the SRM program at the healthcare organization. We found that employees perceived SRM program at the agency as very effective, based on all CSFs except team member empowerment (TME). Both interaction and no interaction effects indicated that perception of employees toward TME was negative. This is an interesting finding of our study. Although it needs to be investigated further, our study has practical implications for managers, as discussed in the earlier section.

With a rise in the use of sophisticated technology in healthcare, there are more risks than an organization can effectively mitigate without a formal SRM program. Therefore, it is imperative that an effective SRM program is in place in a healthcare organization. Information security has been studied in IS. However, the context has been e-commerce and, at best, has been minimally researched [Sharma and Sugumaran, 2011]. While our study contributes to SRM research, there is a need for future research to focus on a holistic approach toward information security incorporating dimensions such as people, technology, and organization.

VII. REFERENCES

Editor's Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the article on the Web, can gain direct access to these linked references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

Adams, A., and A. Blandford (2005) "Bridging the Gap Between Organizational and User Perspectives of Security in the Clinical Domain", *International Journal of Human–Computer Studies,* (63)1, pp. 175–202.

Ahmed, Z., H. Jamal, R. Mehboob, S. Khan, et al. (2010) "Secure Cognitive Mobile Hotspot", *IEEE Transactions on Consumer Electronics*, (56)2, pp. 606–612.

Al-Mashari, M., and M. Zairi (1999) “BPR Implementation Process: An Analysis of Key Success and Failure Factors”, *Business P rocess Management Journal*, (5)1, pp. 87–112.

Blakley, B., E. McDermott, and D. Geer. (2001) “Information Security Is Information Risk Management”, Workshop on New Security Paradigms, Cloudcrodt, New Mexico, 2001, pp. 97–104.

Blumenthal, D. (2010) “Launching HIteCH”, *New England Journal of Medicine,* (362)5, pp. 382–385.

Cisco (2011) “Cisco 2010 Annual Security Report: Highlighting Global Security Threats and Trends”, http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2010.pdf (current February 1, 2011).

DeLone, W., and E. McLean (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.

Dhillon, G., and J. Backhouse (2001) “Current Directions in IS Security Research: Towards Socio-organizational Perspectives”, *Information Systems Journal* (11)2, pp. 127–153.

Dwivedi, A., R.K. Bali, M.A. Belsis, R.N.G. Naguib, et al. (2003) “Towards a Practical Healthcare Information Security Model for Healthcare Institutions”, 4th International IEEE EMBS Special Topic Conference on Information Technology Applications in Biomedicine, UK, 2003, pp. 114–117.

Ein-Dor, P., and E. Segev (1978) “Organizational Context and the Success of Management Information Systems”, *Management Science,* (24)10, pp. 1064–1077.

Eloff, J., and M. Eloff (2005) “Information Security Architecture”, *Computer Fraud & Security,* (2005)11, pp. 10–16.

Epstein, M.A., M.S. Pasieka, W.P. Lord, S.T.C. Wong, et al. (1998) “Security for the Digital Information Age of Medicine: Issues, Applications, and Implementation”, *Journal of Digital Imaging,* (11)1, pp. 33–44.

Farzandipour, M., F. Sadoughi, M. Ahmadi, and I. Karimi (2010) “Security Requirements and Solutions in Electronic Health Records: Lessons Learned from a Comparative Study”, *Journal of Medical Systems,* (34)4, pp. 1–14.

FPA (2007) “The Privacy Act of 1974”, http://www.justice.gov/opcl/privacyact1974.htm (current January 25, 2011).

Gaunt, N. (1998) “Installing an Appropriate Information Security Policy”, *International Journal of Medical Informatics*, (49)1, pp. 131–134.

Giakoumaki, A., K. Perakis, A. Tagaris, and D. Koutsouris (2008) “Digital Watermarking in Telemedicine Applications—Towards Enhanced Data Security and Accessibility”, 8th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, New York, 2008, pp. 6328–6331.

Grumbach, K., and J.W. Mold (2009) “A Health Care Cooperative Extension Service”, *JAMA: The Journal of the American Medical Association*, (301)24, pp. 2589–2591.

HIPAA (1996) “Health Insurance Portability and Accountability Act of 1996”, http://aspe.hhs.gov/admnsimp/pl104191.htm (current January 26, 2011).

Hu, J., and A.C. Weaver (2004) “A Dynamic, Context-aware Security Infrastructure for Distributed Healthcare Applications”, *Proceedings of the First Workshop on Pervasive Security, Privacy and Trust* (PSPT), Boston, MA, 2004.

Jarvenpaa, S., and B. Ives (1991) “Executive Involvement and Participation in the Management of Information Technology”, *MIS Quarterly,* (15)2, pp. 205–227.

Jepsen, T. (2003) “IT in Healthcare: Progress Report”, *IT Professional,* (5)1, pp. 8–14.

Kardas, G., and E.T. Tunali (2006) “Design and Implementation of a Smart Card Based Healthcare Information System”, *Computer Methods and Programs in Biomedicine,* (81)1, pp. 66–78.

Kokolakis, S., and C. Lambrinoudakis (2005) “ICT Security Standards for Healthcare Applications”, *Standardization for ICT Security,* (6)3, p. 47.

Kotulic, A.G., and J.G. Clark (2004) “Why There Aren’t More Information Security Research Studies”, *Information & Management,* (41)5, pp. 597–607.

Lacey, D. (2010) “Understanding and Transforming Organizational Security Culture”, *Information Management & Computer Security,* (18)1, pp. 4–13.

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

Leavitt, N. (2005) “Mobile Phones: The Next Frontier for Hackers?”, *Computer,* (38)4, pp. 20–23.

Lee, A. (1989) “A Scientific Methodology for MIS Case Studies”, *MIS Quarterly,* (13)1, pp. 33–50.

Liu, Y., J.A. Clark, and S. Stepney (2005) “‘Devices Are People Too’: Using Process Patterns to Elicit Security Requirements in Novel Domains: A Ubiquitous Healthcare Example”, *Security in Pervasive Computing,* (3450) 2005, pp. 31–45.

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

Martin, E.W. (1982) “Critical Success Factors of Chief MIS/DP Executives”, *MIS Quarterly,* (6)2, pp. 1–9.

Matuleviius, R., N. Mayer, H. Mouratidis, E. Dubois, et al. (2008) “Adapting Secure Tropos for Security Risk Management in the Early Phases of Information Systems Development”, in Dubois, E., and K. Pohl (eds.), New York: Springer, pp. 541–555.

McCallister, E., T. Glance, and K. Scarfone (2010) *Guide to Protecting the Confidentiality of Personally Identifiable Information,* Gaithersburg, MD: DIANE Publishing.

Mercuri, R. (2004) “The HIPAA-potamus in Health Care Data Security”, *Communications of the ACM,* (47)7, pp. 25–28.

Ng, H., M. Sim, and C. Tan (2006) “Security Issues of Wireless Sensor Networks in Healthcare Applications”, *BT Technology Journal,* (24)2, pp. 138–144.

Page, D. (2010) “A Hospital Imperative: Enterprisewide IT Security”, *Hospitals & Health Networks/AHA,* (84)12, p. 45.

Park, W.S., S.W. Seo, S.S. Son, M.J. Lee, et al. (2010) “Analysis of Information Security Management Systems at 5 Domestic Hospitals with More than 500 Beds”, *Healthcare Informatics Research,* (16)2, pp. 89–99.

Paulson, L. (2002) “Wanted: More Network-security Graduates and Research”, *Computer,* (35)2, pp. 22–24.

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

Ratnasingham, P. (1998) “Trust in Web-based Electronic Commerce Security”, *Information Management and Computer Security*, (6), pp. 162–166.

Renaud, K., and W. Goucher (2012) “Health Service Employees and Information Security Policies: An Uneasy Partnership?”, *Information Management & Computer Security*, (20)4, pp. 296–311.

Rindfleisch, T. (1997) “Privacy, Information Technology, and Health Care”, *Communications of the ACM*, (40)8, pp. 92–100.

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

Sarker, S., and A. Lee (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., K. Lyytinen, M. Keil, and P. Cule (2001) “Identifying Software Project Risks: An International Delphi Study”, *Journal of Management Information Systems*, (17)4, pp. 5–36.

Sharma, S. and V. Sugumaran (2011) "A Framework For Enhancing Systems Security," *Journal of Information Privacy & Security,* (7) 4, pp. 3–22.

Shoniregun, C.A., K. Dube, and F. Mtenzi (2010) “Securing e-Healthcare Information”, in Jajodia, S. (ed.), *Electronic Healthcare Information Security, volume 53,* New York: SpringerLink, pp. 29–57.

Sigler, T.H., and C.M. Pearson (2000) “Creating an Empowering Culture: Examining the Relationship Between Organizational Culture and Perceptions of Empowerment”, *Journal of Quality Management,* (5)1, pp. 27–52.

Smith, J. (2010) “Getting the Right Balance: Information Security and Information Access”, *Legal Information Management,* (10)1, pp. 51–54.

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

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

Su, Y., and L. Al-Hakim (2010) “Assuring Information Quality in Medical Platform for U-Healthcare Service”, IEEE International Conference on Wireless Communications, Networking and Information Security, Beijing, China 2010, pp. 664–668.

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

Zafar, H. (2011) “Security Risk Management at a Fortune 500 Firm: A Case Study”, *Journal of Information Privacy & Security,* (7)4, pp. 23–53.

APPENDIX A

The following questionnaire was used. It has been adapted in its entirety from Zafar [2011].

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

This section highlights the unstructured interview protocol.

Pre-Interview

- Introduce researcher to the participant and briefly mention the purpose of the study.
- Present Informed Consent Form.

Interview

- Conduct an unstructured interview with each participant. Mention to the participant that his/her responses will be recorded.
- Start with an open-ended question about their current position and how the SRM program pertains to them.
- Ask an open-ended question about any situations when SRM hindered their work. Bring up TME.
- Debrief participants about how the interview responses will be used.

Post-Interview

- Create codes and secure all data.
- Summarize some of the memorable things the participant said at different moments.

ABOUT THE AUTHORS

Dr. Humayun Zafar is an Assistant Professor of Information Security and Assurance at Kennesaw State University, Kennesaw, GA. He received his doctorate from the University of Texas at San Antonio. His research interests include organizational security risk management, network security, and organizational performance. Some of his previous work has appeared in journals and conferences such as the *Communications of the AIS, Information Resources Management Journal, Human Resource Management Review, Journal of Emerging Knowledge on Emerging Markets, Journal of Information Privacy & Security, Hawaii International Conference on System Sciences,* and *Americas Conference on Information Systems.*

Dr. Myung Ko is an Associate Professor in the Department of Information Systems & Cyber Security at the University of Texas at San Antonio (UTSA). She received her Ph.D. from Virginia Commonwealth University. Her research interests include the impact of IT on organization, data mining, economics of security breach, and Internet banking. Her work has been published in various refereed journals such as *Information & Management, Information Systems Journal, Decision Support Systems, Information Resources Management Journal, Journal of Information Technology Theory and Application (JITTA),* and *Information Technology & Management.*

Dr. Jan Guynes Clark is a professor of Information Systems at the University of Texas at San Antonio. She received her Ph.D. from the University of North Texas. She is also a Certified Information Systems Security Professional (CISSP). Her research interests include the impact of information technologies on productivity and performance, information security, and IS strategies. Her publications have appeared in leading journals such as *Communications of the AIS, Communications of the ACM, IEEE Transactions on Engineering Management,* and *Information & Management.*

Communications of the Association for Information Systems

ISSN: 1529-3181

Communications of the Association for Information Systems