2017

The Effect of Perceived System Risks on HIS Misuse Intention: The Role of System Resilience under the Context of Disasters

Dheyaaldin Alsalman
Dakota State University

Insu Park
Dakota State University

The Effect of Perceived System Risks on HIS Misuse Intention: The Role of System Resilience under the Context of Disasters

Emergent Research Forum Paper

Dheyaaldin Alsalman
Dakota State University
Madison, SD 57042
Diya2060@hotmail.com

Insu Park
Dakota State University
Madison, SD 57042
Insu.park@dsu.edu

Abstract

Although, the usage of healthcare information systems (HIS) has provided many potential benefits such as enhancing the availability, accessibility and readability of information, healthcare information security has become a growing public concern. Most of the studies have shown the importance of sanctions, information security policy, and information awareness programs in reducing IS misuse behavior, but individuals may still tend to engage in inappropriate behaviors, especially under the context of disasters. The vulnerabilities and risks associated with the HIS could be very extreme under disasters, which may cause employees to misuse their HIS for the sake of delivery of health services and business continuity. In this case, we believe that system resilience, which is the ability of the HIS to adapt to unexpected disruptions could play a role in encouraging them not to act inappropriately and engage in misuse behaviors.

Keywords

Perceived system risk, perceived system resilience, HIS misuse intention, disaster context.

Introduction

Even though earlier empirical studies have shown the importance of sanctions, information security policy, and information awareness programs in reducing IS misuse behavior (Bulgurcu et al. 2010; Kankanhalli et al. 2003; Pahnila et al. 2007), individuals may still tend to engage in inappropriate behaviors. It may be because individuals' decision to misuse may be different across various situations they are placed. For instance, unlike normal situation, disasters can create damage and reduce access to information (Amaratunga et al. 2009), increase difficulties for communication and collaboration (Lizarralde and Massyn 2008), or increase employees' stress levels and perceptions of system risk, which in turn negatively affects the image of the organization's capabilities (Park et al. 2015). The vulnerabilities and risks associated with the healthcare information system (HIS) could be very extreme under disasters, which may cause employees to act inappropriately for the sake of delivery of health services and business continuity.

Despite these various situations bring potential threats for misusing IS, there is still a lack of investigations on how individuals are involved in misusing information systems in different contexts, specifically disaster context. In the context of disasters, it should be true that employees may intend to misuse their HIS due to the motivation of necessary defense. This could occur due to their high perception of system risks caused by the vulnerabilities and risks associated with the HIS. Under the context of disasters, such loss of access to information could be very extreme because it can disrupt clinical and business processes, which can potentially have far-reaching effects such as patient injury, legal liability, and significant financial loss to the organization (Paustian et al. 2002). Hence, the inability of the HIS to ensure information availability could increase employees' perceived system risks, which could in turn

impact their behavior (Heal and Kunreuther 2007) and negatively influence their performances (Park et al. 2015). As a result, employees may simply intend to misuse their HIS if doing so could help them to do their jobs for the sake of delivery of health services and business continuity. This leads us to the first research question: How does perceived system risk affect employees' intention to misuse the healthcare information system (HIS) under the context of disasters? Employees who are authorized to use the HIS may sometimes jeopardize the information security because of their ignorance, mistakes, and deliberate acts (Lee et al. 2004). In this case, system resilience, which is the ability of the healthcare information system (HIS) to adapt to unexpected disruptions (Park et al. 2015), has been little studied whether it can play a role in reducing their HIS misuse behavior under the context of disasters. This leads us to the second research question: Does system resilience encourage employees not to misuse the healthcare information system (HIS) during disaster situations?

The purpose of this study is to investigate the effect of perceived system risk (urgency) on employees' HIS misuse during disaster situations. More importantly, we aim to examine the moderating role of system resilience on employees' misuse. Increasing resilience, which is defined as the capability to deal with unexpected events, could lower the negative consequences of extreme events (Heal and Kunreuther 2007). Thus, in this study, we propose that system resilience would play a buffering role in reducing the effect of perceived system risks on misuse behavior, especially under disaster situations.

Literature: Healthcare Information System (HIS) Misuse

Organizations define IS misuse as misuse of IS resources (Magklaras and Furnell 2001). Since the domain of HIS misuse is quite varied that ranges from behaviors that are unethical and/or inappropriate to those that are illegal, we attempt to examine a range of HIS misuse behaviors in various contexts by focusing on four HIS misuses: (1) sharing passwords, (2) unauthorized disclosure of confidential information, (3) unauthorized access to restricted information, (4) inappropriate usage of email in the workplace. Sharing passwords has been identified as one of the major security issues that can lead to a loss of confidence about hospitals' ability to stick to HIPAA guidelines. This is consistent with the interview with the chief operating officer of a hospital that was affected by the October 2006 snowstorm of western New York,

> *"Hospital employees with access to information regarding certain patients did not report to work because the snow storm caused the roads to become unpliable and a driving ban went into effect…. They shared passwords among themselves….This was in part a reason for a loss of confidence [by HIS users] about the IT department's ability to stick to HIPAA guidelines" (in Park, Sharman, & Rao, 2015, p. 319).*

In addition, unauthorized access to computerized data has been reported as one of the most common types of breaches in organizations (Richardson 2007). Furthermore, inappropriate usage of email in the workplace has been shown to place organizations at financial or legal risk (D'Arcy et al. 2009). Although these four behaviors do not count all possible IS misuse types, we consider them as representative of typical IS misuse issues often encountered by organizations, which include accessibility, privacy, property, and accuracy (Mason 1986). We believe that these four inappropriate behaviors could be maximized in hospital context, especially during disaster situations. For instance, disasters can reduce access to information (Amaratunga et al. 2009), increase difficulties for communication and collaboration (Lizarralde and Massyn 2008), increase pressure to act quickly, and place responders at risk (Kathleen Geale 2012). In this case, employees will be unable to perform their job due to this context, which can lead to increase their stress levels and perceptions of system risk (Park et al. 2015). Thus, for patient safety and quality health care, and the organizational business continuity, they may simply intend to misuse their HIS since they are required to act quickly under this urgent situation. Taking this into consideration, under normal situations, employees' IS misuse behavior causes damage and is viewed as a crime in a society, therefore earlier empirical studies have focused on deterrent and preventative strategies (e.g., sanctions) for reducing IS misuse (Bulgurcu et al. 2010; Kankanhalli et al. 2003; Pahnila et al. 2007). Generally, there is no possible legitimate reason behind this IS misuse behavior, but in the case of HIS misuse behavior under disaster context, however, high perception of system risks, disruption of delivery of health services and business continuity are very legitimate and important reasons for employees. Thus, deterrence theory may not provide sufficient explanations about employees' HIS misuse behavior under the context of disasters without a consideration of the legitimate reasons behind it. Hence, understanding employees' HIS misuse behavior under disaster context is still limited.

Hypotheses Development

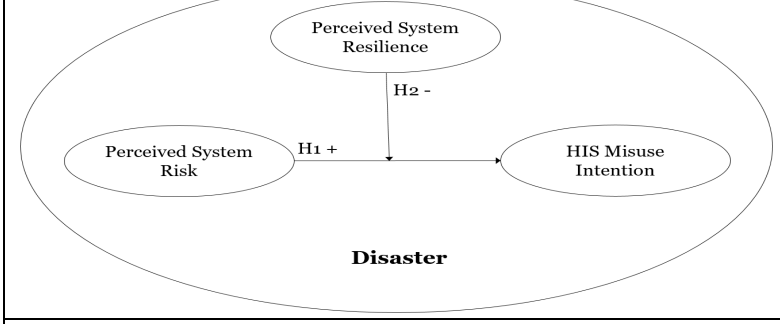

Figure 1. The Proposed Model

Perceived System Risk

Perceived system risk is employees' subjective expectations and assessments of the risk caused by damage or loss to information systems (Straub and Welke 1998). In this study, this perception of system risk could appear when employees perceive that their healthcare information system (HIS) is detrimentally affected (Heal and Kunreuther 2007). Basically, when any loss or disruption of HIS occurs, system risk would be impacted. We focus on perceived system risk as a specific concept that has not been discussed in the context of HIS misuse in prior IS literature, although it has been discussed with regard to perceived HIS usefulness (Park et al. 2015). In the context of HIS, especially under disaster situations, it could have a detrimental effect on employees' HIS misuse intention, as system risk may hinder the use of HIS. Since disasters can create damage and cause a loss of all or a portion of the healthcare information system (HIS) functionality (Paustian et al. 2002), employees will be unable to access information, share information and communicate with their colleagues. In this case, employees will perceive their HIS ineffective and incapable in supporting their jobs under disasters, which will increase their perceived system risk that would in turn decrease their perception of HIS usefulness (Park et al. 2015). Thus, this situation derived from perceived system risk may lead employees to limited behavioral options to complete their jobs by dealing with unexpected events. Due to employees' fear to lose clinical and business processes, their high perception of system risk could impact their behavior (Heal and Kunreuther 2007) and negatively influence their performances (Park et al. 2015). As a result, for the sake of delivery of health services and business continuity, employees may attempt to act inadequately such as sharing passwords, accessing unauthorized and restricted information, and disclosing information if doing so can help them to do their jobs. We argue that high level of perceived system risks would positively impact employees' HIS misuse behavior, therefore we follow a recent study that shows perceptions, beliefs, and even emotions can affect users' IS use behavior (Beaudry and Pinsonneault 2010). Thus, we hypothesize:

Hypothesis 1: *Perceived system risk positively affects employees' intention to misuse the healthcare information system (HIS).*

Perceived System Resilience

In the health care area, successful management of HIS is crucial for delivery of health services, employees' performance, and business performance of the organization. The state of hospitals can be vulnerable if the HIS is affected by the disasters because all health practices and business processes rely on the availability of access to information, information sharing, and communication. Prior studies have provided evidence suggesting that poor information sharing and coordination has a negative influence on collective decision-making and actions during disaster response (Helsloot 2005; Junglas and Ives 2007; Pan et al. 2005). Therefore, it is important to ensure the functionality of the HIS because access to information can enhance the efficiency and effectiveness of responses (Horan and Schooley 2007).

Hospitals should ensure access to information by increasing their system resilience, which is its ability to adapt to and recover quickly from unexpected disruptions, which would include business continuity, disaster recovery (Park et al. 2015), and IT systems configuration (Nemeth et al. 2008). We argue that

system resilience can play an important role in ensuring access to information, which will facilitate the process of information sharing and communication, and then enhance employees' decision-making process and actions. Hence, if hospitals have healthcare information systems (HIS) that are being resilient enough to handle unexpected events by ensuring access to information, employees will make better decisions and act positively, which in turn leads to reduce their HIS misuse intention. Thus, we hypothesize:

Hypothesis 2: *The effect of perceived system risk on employee's intention to misuse the healthcare information system (HIS) will be weakened by perceived system resilience.*

Proposed research method

Method

We will use the survey method to test our proposed model. The survey will be conducted in multiple hospitals that were affected by disasters via a crowdsourcing company such as Qualtrics (qualtrics.com). The subjects must be involved in related HIS tasks with access to organizational data. We developed the initial survey instrument by identifying appropriate measurement scales that were adapted from the existing measures used in prior studies that were proved reliable and valid. Data will be collected by administering the final survey instrument online.

Constructs	**Definitions**	**Items (reference)**
Perceived System Risk	Subjective expectations and assessments of the risks caused by the loss or disruption of the healthcare information systems (HIS) (Straub and Welke 1998).	4 items modified from (Bulgurcu et al. 2010)
Perceived System Resilience	Individual's belief regarding the capacity of their information systems to maintain and cope with damages or losses (Rose 2004).	4 items (New)
HIS Misuse Intention	Employees' intention to share passwords, access unauthorized restricted information, disclose unauthorized information, and use email inappropriately in the organization.	2 items modified from (D'Arcy et al. 2009) 2 items (New)

Table 1. Definitions and Sources of Measurement Items

Data Analysis

Structural equation modeling (SEM), as implemented in SPSS, will be used for data analysis. The SEM approach allows researchers to examine relationships among multiple variables simultaneously. It is an effective multivariate technique for testing theories due to its applications of causal modeling and confirmatory factor analysis (CFA) (Hair et al. 2006). Since our study was primarily intended for casual-predictive analysis, SEM is an appropriate statistical tool because it focuses a prediction-oriented and data analytic method, seeking to test the entire model and measure it overall (Hair et al. 2006).

Conclusion and Contribution

This paper provides a conceptual framework explaining the effect of perceived system risks on healthcare information system (HIS) misuse intention, extending the body of research on the importance of system resilience, and allowing integration of insights in the context of disasters. The contribution of this paper to the literature on healthcare information system (HIS) misuse intention is that it demonstrates the importance of perceived system risk as a factor impacting healthcare information system (HIS) misuse intention as well as the importance of system resilience as a moderating variable impacting the relationship between perceived system risk and healthcare information system (HIS) misuse intention.

Acknowledgement: The second author was supported by South Dakota Board of Regents competitive grant (SDBOR/ DSU 2016-06-02).

References

Amaratunga, D., Haigh, R., Thanurjan, R., and Indunil P. Seneviratne, L. 2009. "The Role of Knowledge Management in Post-Disaster Housing Reconstruction," *Disaster Prevention and Management: An International Journal* (18:1), pp. 66-77.

Beaudry, A., and Pinsonneault, A. 2010. "The Other Side of Acceptance: Studying the Direct and Indirect Effects of Emotions on Information Technology Use," *MIS quarterly*), pp. 689-710.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS quarterly* (34:3), pp. 523-548.

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

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., and Tatham, R. L. 2006. *Multivariate Data Analysis*. Pearson Prentice Hall Upper Saddle River, NJ.

Heal, G., and Kunreuther, H. 2007. "Modeling Interdependent Risks," *Risk Analysis* (27:3), pp. 621-634.

Helsloot, I. 2005. "Bordering on Reality: Findings on the Bonfire Crisis Management Simulation," *Journal of Contingencies and Crisis Management* (13:4), pp. 159-169.

Horan, T. A., and Schooley, B. L. 2007. "Time-Critical Information Services," *Communications of the ACM* (50:3), pp. 73-78.

Junglas, I., and Ives, B. 2007. "Recovering It in a Disaster: Lessons from Hurricane Katrina," *MIS Quarterly Executive* (6:1).

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

Kathleen Geale, S. 2012. "The Ethics of Disaster Management," *Disaster Prevention and Management: an international journal* (21:4), pp. 445-462.

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

Lizarralde, G., and Massyn, M. 2008. "Unexpected Negative Outcomes of Community Participation in Low-Cost Housing Projects in South Africa," *Habitat International* (32:1), pp. 1-14.

Magklaras, G., and Furnell, S. 2001. "Insider Threat Prediction Tool: Evaluating the Probability of It Misuse," *Computers & Security* (21:1), pp. 62-73.

Mason, R. O. 1986. "Four Ethical Issues of the Information Age," *Mis Quarterly*), pp. 5-12.

Nemeth, C., Wears, R., Woods, D., Hollnagel, E., and Cook, R. 2008. "Minding the Gaps: Creating Resilience in Health Care,").

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' Behavior Towards Is Security Policy Compliance," *System sciences, 2007. HICSS 2007. 40Th annual hawaii international conference on*: IEEE, pp. 156b-156b.

Pan, S. L., Pan, G., and Devadoss, P. 2005. "E-Government Capabilities and Crisis Management: Lessons from Combating Sars in Singapore,").

Park, I., Sharman, R., and Rao, H. R. 2015. "Disaster Experience and Hospital Information Systems: An Examination of Perceived Information Assurance, Risk, Resilience, and His Usefulness," *Mis Quarterly* (39:2), pp. 317-344.

Paustian, P. E., Slovensky, D. J., and Kennedy, J. W. 2002. "Information System Failures in Healthcare Organizations: Case Study of a Root Cause Analysis," in *Effective Healthcare Information Systems*. IGI Global, pp. 231-236.

Richardson, R. 2007. "Csi," *FBI Computer Crime and Security Survey*).

Rose, A. 2004. "Defining and Measuring Economic Resilience to Disasters," *Disaster Prevention and Management* (13:4), p. 307.

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