2018

The Determinant of Selfless Misuse Intention and the Role of System Resilience under the Context of Disasters

Insu Park

Dheyaaldin Alsalman

The Determinant of Selfless Misuse Intention and the Role of System Resilience under the Context of Disasters

Emergent Research Forum (ERF)

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

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

Abstract

The extant literature has investigated how individuals engage in inappropriate behaviors based on the rational choice theory (RCT), and the neutralization theory under normal situations, however it has given little consideration to how individuals engage in inappropriate behaviors under the context of disasters. To fill this research gap, we propose a selfless misuse model, which offers a theoretical explanation for the impact of the concept of bounded rationality on individuals' selfless misuse intention under the context of disasters. In addition, to reduce this misuse behavior, we aim to investigate the role of system resilience in assisting employees to make better decisions and act positively.

Keywords

Selfless misuse, bounded rationality, intrinsic cost, intrinsic benefit, perceived system resilience.

Introduction

Employees' abuse and misuse of IS resources have been considered as the major information security issue related to insiders since employees are assumed to simply choose to engage in inappropriate behaviors (Bulgurcu et al. 2010). For instance, in a recent study (Hu et al. 2011), it was found that individuals intend to commit violations (e.g., computer misconduct) based on their assessment of perceived intrinsic benefits and perceived intrinsic costs. In another study (Siponen and Vance 2010), it was found that employees intend to violate IS security policies based on several neutralization techniques (e.g., defense of necessity). These might be considered as several types of insider threats to disrupt their information systems under normal situations. However, even though we consider these types of behavior could be a motivation for individuals to misuse, individuals' decision to misuse may be different across various situations they are placed. Disasters can create damage and reduce access to information (Amaratunga et al. 2009), increase difficulties for communication and collaboration (Lizarralde and Massyn 2008), and 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). Some types of disasters can include hurricanes, earthquakes, floods, and tsunamis. Thus, the vulnerabilities and risks associated with the healthcare information system (HIS) could be very extreme under these disasters, which can place employees in unfamiliar situations that demand timely actions. Hence, due to these urgent situations, employees may act with limited rational decision making process and intend to engage in misuse as a "good enough" solution (Simon 1996) for the sake of delivery of health services and business continuity. Because individuals tend to act altruistically when experiencing natural disasters (i.e., giving, helping and sharing) (Li et al. 2013), misusing IS resources for them to conduct their work is more likely to be their responsibility even though their behaviors should not be encouraged to do so. Thus, in this study, HIS misuse would reflect a bright aspect of general misuse concept (i.e., selfless misuse) which is brought by contextual boundary. Although, the extant literature has investigated how individuals engage in inappropriate behaviors based on the rational choice theory (RCT)

(e.g., computer misconduct) and the neutralization theory (e.g., IS security policies violation) under normal situations, it has given little consideration to how individuals are involved in this *selfless misuse* of information systems to perform their tasks under the context of disasters. This gap leads to a further examination of the factors impacting employees' intention to misuse HIS during disaster situations. This leads us to the first research question: (1) What are the factors that affect employees' selfless misuse intention in the context of disasters? Since the primary job of most organizations is to develop strategies to reduce the probabilities of negative events (Heal and Kunreuther 2007) in order to manage uncertainty to achieve performance, we believe that system resilience can play a key role in reducing an organization's vulnerability and lowering the negative consequences of extreme events (Heal and Kunreuther 2007). In addition, (2) How does system resilience affect employees' selfless intention to misuse HIS during disaster situations? These questions point toward an overall goal of the current study, which is to understand the way of employees' selfless misuse behavior and examine the role of system resilience in the context of disasters.

Literature: Conceptualization of Selfless Misuse

In general, IS misuse refers to individuals' inappropriate behavior in using IS resources (Magklaras and Furnell 2001). However, in disaster context, individuals' misuse behavior highly likely appears in different aspects from normal situations. 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). This urgent situation can affect the way individuals act as they normally do under normal situations and may force them to make quick decisions to behave. This is consistent with the concept of bounded rationality as risk and uncertainty may affect the way individuals make decisions while lack of information may pose a considerable limitation on their decision-making process (Simon 1972). Therefore, individuals in this view act as satisfiers who aim to seek a solution that can be considered "good enough" while considering the effort required to obtain it and the resources available (Simon 1996). In this case, due to individuals' irrational or limited rational thinking, they may decide to misuse HIS as a good enough solution for the sake of delivery of health services and business continuity. Because individuals tend to act altruistically when experiencing natural disasters (i.e., giving, helping and sharing) (Li et al. 2013), in this study, HIS misuse would reflect a bright aspect of general misuse concept which is brought by contextual boundary. Based on the bright side of misuse, we use the term 'selfless misuse', which is defined as the behaviors engaged in by employees who misuse HIS with a strong intention to do good.

Hypotheses Development

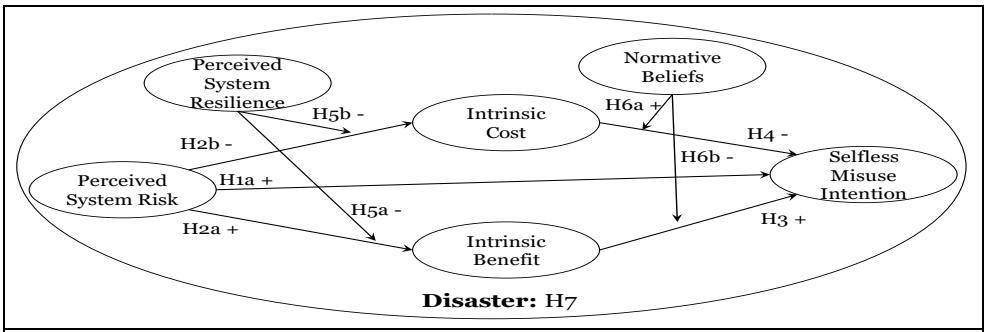

Figure 1. The Proposed Model

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). 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. Thus, for the sake of delivery of

health services and business continuity, employees may attempt to act altruistically and selflessly misuse their HIS if doing so can help them to do their jobs, especially under extreme and urgent situations.

Hypothesis 1a: *Perceived system risk will increase employees' selfless misuse intention under disaster context.*

Hypothesis 2a-b: *Perceived system risk increases (2a) (decreases (2b)) employees' intrinsic benefits (costs) of selfless misuse under disaster context.*

Intrinsic Cost and Benefit

Intrinsic cost and benefit are intrinsic motivations that can help employees justify their actions associated with HIS in terms of internal reasons, such as their own inspirations under the context of disasters. The literature shows that individuals are sensitive to the consequences of their actions and make reasoned judgements based on the cost-benefit analysis of the intended acts (Becker 1968; Cornish and Clarke 2014; Paternoster and Simpson 1996). However, under the context of disasters, this cost-benefit approach is used differently than it is under normal situations. Disasters can decrease the perceived self-competence and self-esteem of individuals (Wolfenstein 1957), therefore those affected by them may simply act by making sense of motivations (Coopey et al. 1997), which can be considered an evaluation of intrinsic costs and intrinsic benefits in our study to respond to their identity needs (e.g., self-competence and self-esteem). Since Weick (2005) argues that individuals tend to do sense-making in order to meet their general long-term goals, we believe that employees may act based on the importance of delivery of health services and business continuity that may lead to their organizational commitment or altruism in the organization. Hence, we posit that employees' intrinsic benefits of selfless misuse may dominate their intrinsic costs for the purpose of meeting their general long-term goals as well as their identity needs. Thus, we hypothesize:

Hypothesis 3: *Employees' intrinsic benefit is positively associated with their selfless misuse intention.*

On the other hand, employees should perceive that there is a cost associated with IS misuse intention because based on the deterrence theory, prior studies have shown that sanctions are so effective in deterring crimes related to computer security (Kankanhalli et al. 2003; Pahnila et al. 2007). Hence, employees' intrinsic costs may decrease their motivations to act inappropriately or illegally in their decision-making process, which may discourage them to misuse the healthcare information system (HIS). Thus, we hypothesize:

Hypothesis 4: *Employees' intrinsic cost is negatively associated with their selfless misuse intention.*

Perceived System Resilience

Past studies show that ensuring the functionality of HIS is important for individuals to access information that can enhance the efficiency and effectiveness of responses (Comfort et al. 2004; Horan and Schooley 2007). Thus, hospitals should ensure access to information by increasing their system resilience, which is its ability to adapt to and recover quickly from unexpected disruptions. Resilience has been shown to play an important role in the reduction of the consequences of negative events (Heal and Kunreuther 2007) as well as organizational vulnerabilities. Hence, if hospitals have a resilient HIS to handle unexpected events by ensuring access to information, employees will make better decisions and act positively, which in turn leads to increase their intrinsic costs and decrease their intrinsic benefits of selfless misuse intention, especially when the perceived benefits of HIS is high. Thus, we hypothesize:

Hypothesis 5a-b: *The positive (5a) (negative (5b)) relationship between perceived system risk and employee's intrinsic benefits (costs) will be weakened by perceived system resilience.*

Normative Beliefs

According to a recent study, employees' normative beliefs significantly affect their intention to comply with the requirements of the information security policy (ISP) (Bulgurcu et al. 2010). In line with the existing literature, we posit that the relationships between employees' intrinsic benefits, employees' intrinsic costs, and their selfless intentions to misuse HIS are associated with employees' normative beliefs.

Hypothesis 6a-b: *The negative (6a) (positive (6b)) relationship between intrinsic costs (benefits) and selfless misuse intention will be strengthened (weakened) with employee's normative beliefs.*

Disaster Effect

Since extreme events 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), individuals act within high levels of uncertainty, which gives them no choice between satisfactory and optimal solutions except accepting a "good enough" solution (Simon 1996). In this case, any disruption of clinical and business processes would bring employees' intention to misuse HIS for the sake of delivery of health services and business continuity. Thus, under the context of disasters, employees' perceived intrinsic benefits will be more influential on their selfless misuse intention than under normal situations because they are acting with limited rationality.

Hypothesis 7: *Under the context of disasters, employees' selfless misuse intention will be higher than under normal situations.*

Proposed Research Method

We will use the survey method to test our proposed model. The survey will be conducted in multiple hospitals located in disastrous areas. 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 HIS.	4 items (Bulgurcu et al. 2010)
Intrinsic Benefit	Positive feelings, such as satisfaction, accomplishment, fulfillment, and contentment.	4 items (Bulgurcu et al. 2010)
Intrinsic Cost	Negative feelings, such as stress, guilt, shame, and embarrassment.	4 items (Bulgurcu et al. 2010)
Perceived System Resilience	Beliefs regarding the capacity of the information systems to maintain and cope with damages or losses (Rose 2004).	4 items (New)
Normative Beliefs	Perceived social pressure caused by behavioral expectations of such important referents as managers, colleagues, and executives.	3 items (Ajzen 1991)
Selfless Misuse Intention	Intention to misuse HIS to do good.	2 items (D'Arcy et al. 2009) 2 items (New)

Table 1. Definitions and Sources of Measurement Items

Expected Contributions and Next Step

Drawing on the concept of bounded rationality, this study makes a significant contribution by offering a new theoretical perspective to advance our understanding of employees' motivations to engage in HIS misuse behavior in addition to what was offered by the rational choice theory (RCT) and neutralization theory perspectives. Also, this study demonstrates the importance of system resilience as a moderating variable in the reduction of selfless misuse intention. Our next step is to use partial least squares (PLS) for data analysis because it focuses on a prediction-oriented and data-analytic method, seeking to maximize the variances that are explained in the constructs (Barclay et al. 1995).

References

Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational behavior and human decision processes* (50:2), pp. 179-211.

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.

Barclay, D., Higgins, C., and Thompson, R. 1995. "The Partial Least Squares (Pls) Approach to Causal Modeling: Personal Computer Adoption and Use as an Illustration," *Technology studies* (2:2), pp. 285-309.

Becker, G. S. 1968. "Crime and Punishment: An Economic Approach," in *The Economic Dimensions of Crime*. Springer, pp. 13-68.

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.

Comfort, L. K., Ko, K., and Zagorecki, A. 2004. "Coordination in Rapidly Evolving Disaster Response Systems: The Role of Information," *American Behavioral Scientist* (48:3), pp. 295-313.

Coopey, J., Keegan, O., and Emler, N. 1997. "Managers' Innovations as 'Sense-Making'," *British Journal of Management* (8:4), pp. 301-315.

Cornish, D. B., and Clarke, R. V. 2014. *The Reasoning Criminal: Rational Choice Perspectives on Offending*. Transaction Publishers.

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.

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

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

Hu, Q., Xu, Z., Dinev, T., and Ling, H. 2011. "Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?," *Communications of the ACM* (54:6), pp. 54-60.

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.

Li, Y., Li, H., Decety, J., and Lee, K. 2013. "Experiencing a Natural Disaster Alters Children's Altruistic Giving," *Psychological science* (24:9), pp. 1686-1695.

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.

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.

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.

Paternoster, R., and Simpson, S. 1996. "Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime," *Law and Society Review*), pp. 549-583.

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.

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

Simon, H. A. 1972. "Theories of Bounded Rationality," *Decision and organization* (1:1), pp. 161-176.

Simon, H. A. 1996. *The Sciences of the Artificial*. MIT press.

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

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

Weick, K. E., Sutcliffe, K. M., and Obstfeld, D. 2005. "Organizing and the Process of Sensemaking," *Organization science* (16:4), pp. 409-421.

Wolfenstein, M. 1957. *Disaster: A Psychological Essay*. Free Press and Falcon's Wing Press.