

Summer 7-2018

## Is Information Systems Misuse Always Bad? A New Perspective on IS Misuse in Hospitals Under the Context of Disasters

Dheyaaldin Alsalman  
*Dakota State University*

Follow this and additional works at: <https://scholar.dsu.edu/theses>



Part of the [Business Analytics Commons](#), [Databases and Information Systems Commons](#), [Health Information Technology Commons](#), and the [Information Security Commons](#)

---

### Recommended Citation

Alsalman, Dheyaaldin, "Is Information Systems Misuse Always Bad? A New Perspective on IS Misuse in Hospitals Under the Context of Disasters" (2018). *Masters Theses & Doctoral Dissertations*. 340.  
<https://scholar.dsu.edu/theses/340>

This Dissertation is brought to you for free and open access by Beadle Scholar. It has been accepted for inclusion in Masters Theses & Doctoral Dissertations by an authorized administrator of Beadle Scholar. For more information, please contact [repository@dsu.edu](mailto:repository@dsu.edu).



**IS INFORMATION SYSTEMS MISUSE ALWAYS BAD?  
A NEW PERSPECTIVE ON IS MISUSE IN HOSPITALS  
UNDER THE CONTEXT OF DISASTERS**

A dissertation submitted to Dakota State University in partial fulfillment of the requirements  
for the degree of

Doctor of Science

in

Information Systems

07, 2018

By

Dheyaaldin Alsalman

Dissertation Committee:

Dr. Insu Park

Dr. David Zeng

Dr. Yen-Ling Chang



## DISSERTATION APPROVAL FORM

This dissertation is approved as a credible and independent investigation by a candidate for the Doctor of Science in Information Systems degree and is acceptable for meeting the dissertation requirements for this degree. Acceptance of this dissertation does not imply that the conclusions reached by the candidate are necessarily the conclusions of the major department or university.

Student Name: Dheyaaldin Alsalman

Dissertation Title: Is Information Systems Misuse Always Bad? A New Perspective on IS Misuse in Hospitals under the Context of Disasters

Dissertation Chair/Co-Chair: *Insu Park* Date: 07/25/2018

Dissertation Chair/Co-Chair: \_\_\_\_\_ Date: \_\_\_\_\_

Committee member: *David Zeng* Date: 7/25/18

Committee member: *Yenling Chang* Date: 7/26/2018

Committee member: \_\_\_\_\_ Date: \_\_\_\_\_

Committee member: \_\_\_\_\_ Date: \_\_\_\_\_

## **ABSTRACT**

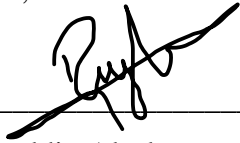
Although the extant literature has investigated how individuals engage in inappropriate behaviors based on the rational choice theory (RCT) (e.g., computer misconduct), the neutralization theory (e.g., IS security policies violation), and workarounds under normal situations, it has given little consideration to how individuals are involved in misuse of information systems with a good intention under the context of disasters. To fill this research gap, we propose a selfless misuse model, which offers a theoretical explanation for the concept of individuals' selfless misuse intention under uncertainty caused by disasters. In this study, we show why employees make decisions to misuse the information system to ensure delivery of health services and business continuity. In addition, we explore the way of reducing this misuse behavior by introducing the role of system resilience in assisting employees to make better decisions and act positively.

## DECLARATION

I hereby certify that this dissertation constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions or writings of another.

I declare that the dissertation describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,

A handwritten signature in black ink, appearing to read 'Dheyaaldin Alsalman', is written over a horizontal line.

Dheyaaldin Alsalman

# TABLE OF CONTENTS

<b>DISSERTATION APPROVAL FORM.....</b>	<b>II</b>
<b>ABSTRACT .....</b>	<b>III</b>
<b>DECLARATION .....</b>	<b>IV</b>
<b>TABLE OF CONTENTS .....</b>	<b>V</b>
<b>LIST OF TABLES.....</b>	<b>VII</b>
<b>LIST OF FIGURES.....</b>	<b>VIII</b>
<b>INTRODUCTION .....</b>	<b>1</b>
BACKGROUND OF THE PROBLEM .....	1
STATEMENT OF THE PROBLEM .....	2
OBJECTIVES OF THE PROJECT .....	3
<b>THEORETICAL BACKGROUND .....</b>	<b>3</b>
RATIONAL CHOICE THEORY (RCT).....	4
NEUTRALIZATION THEORY .....	5
PROTECTION MOTIVATION THEORY (PMT) .....	6
DETERRENCE THEORY .....	7
WORKAROUNDS .....	8
BOUNDED RATIONALITY UNDER EXTREME EVENTS .....	9
UNCERTAINTY FROM DISASTERS .....	10
COST-BENEFIT APPROACH.....	10
<b>LITERATURE REVIEW .....</b>	<b>12</b>
PERCEIVED SYSTEM RISK .....	12
SYSTEM RESILIENCE.....	12
CONCEPTUALIZATION OF SELFLESS MISUSE UNDER DISASTER CONTEXT .....	14
<b>MODEL DEVELOPMENT AND HYPOTHESES .....</b>	<b>16</b>
PERCEIVED SYSTEM RISK .....	16
PERCEIVED SYSTEM RESILIENCE .....	18
UNCERTAINTY .....	19
INTRINSIC COST AND BENEFIT.....	20
CONTROL VARIABLES .....	21
<b>RESEARCH METHODOLOGY .....</b>	<b>22</b>

<b>DATA ANALYSES AND RESULTS.....</b>	<b>25</b>
DATA ANALYSIS.....	25
COMMON METHOD BIAS .....	25
MEASUREMENT MODEL.....	25
STRUCTURAL MODEL TESTING.....	27
POST-HOC ANALYSIS .....	28
<b>DISCUSSION AND IMPLICATIONS .....</b>	<b>28</b>
DISCUSSION.....	28
THEORETICAL CONTRIBUTIONS .....	30
PRACTICAL IMPLICATIONS.....	31
<b>LIMITATIONS, FUTURE RESEARCH, AND CONCLUSIONS.....</b>	<b>32</b>
<b>REFERENCES .....</b>	<b>33</b>
<b>APPENDIX A.....</b>	<b>38</b>

## LIST OF TABLES

Table 1. Definitions and Sources of Measurement Items .....	23
Table 2. Demographic Characteristics of Respondents .....	24
Table 3. Full Collinearity VIFs .....	25
Table 4. Inter-construct Correlation.....	26
Table 5. Cross-Loadings .....	26
Table A1. Survey Questions .....	38



## LIST OF FIGURES

Figure 1. The Proposed Model.....	16
Figure 2. Results of Data Analysis.....	27

# CHAPTER 1

## INTRODUCTION

### **Background of the Problem**

Hospitals' information systems have been shown to be exposed to internal (e.g., inadequate behavior) (Gordon et al. 2005) and external threats (e.g., extreme incident), and that more than three-quarters of security breaches were resulted from inside activity (Ernst and Young 2002). Especially, 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), individuals intend to commit violations (e.g., computer misconduct) based on their assessment of perceived intrinsic benefits and perceived intrinsic costs. The results suggest that their perceived intrinsic benefits dominate their perceived intrinsic costs in the rational decision-making process, therefore individuals' intrinsic satisfactions (e.g., thrill and happiness) gained from the misconduct are very influential on individuals' behavioral choice. 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). Additionally, many studies have found that when employees experience difficulties in working around operational failures in a policy-compliant manner, they will engage in risky workarounds to complete their tasks (Ash et al. 2004; Halbesleben et al. 2008; Holden et al. 2013; Koppel et al. 2008). 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 to be motivations for individuals to misuse, individuals' decision to misuse may be different across various situations they are placed. In this study, we argue that individuals' intention to misuse relies on their intrinsic motivations as out of interest, which are used as intrinsic benefit (e.g., accomplishment) and intrinsic cost (e.g., stress).

Interestingly, in extreme situations, employees in hospitals can spark their intrinsic motivations for their decision making to misuse HIS differently from normal situations.

Individuals make poor decisions about disaster management due to psychological, organizational, and economic reasons (Michel-Kerjan and Slovic 2010), and they tend to act altruistically when experiencing natural disasters (i.e., giving, helping and sharing) (Li et al. 2013). Since disaster situations can place employees in unfamiliar situations that demand timely actions so that increase their uncertainty. Due to uncertainty from 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. In this case, 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. This phenomenon shows the bright aspect of general misuse concept (i.e., selfless misuse) which is brought by contextual boundary.

### **Statement of the problem**

The extant literature has only investigated how individuals engage in inappropriate behaviors based on the rational choice theory (RCT) (e.g., computer misconduct) (Hu et al. 2011), the neutralization theory (e.g., IS security policies violation) (Siponen and Vance 2010), and workarounds (Ash et al. 2004; Halbesleben et al. 2008; Holden et al. 2013; Koppel et al. 2008) under normal situations. Despite the numerous research on the dark side of malicious misuse, however, 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 unexplored area leads to research questions for further examination of employees' HIS misuse during disaster situations: (1) What makes employees selflessly misuse their hospital information systems under disaster situations? We consider perceived system risk and resilience, which are considered as two sides of one coin, as main factors affecting organizations' vulnerability (Sheffi and Rice Jr 2005) and the negative/positive consequences of extreme events (Heal and Kunreuther 2007). In addition, (2) How do employees' intrinsic cost and benefit influence their decision making to selflessly misuse HIS and intermediate the two factors on selfless misuse in disaster situations?

## **Objectives of the project**

The goal of this study is to understand the way of employees' selfless misuse behavior by incorporating intrinsic cost and benefit under the context of disasters. Specifically, we investigate the effect of perceived system risk and resilience on employees' HIS selfless misuse. Second, drawing on the bounded rationality (Cornish and Clarke 1986), we examine how employees' intrinsic cost and benefit are affected by uncertainty causing the bounded rationality, and how they work together to mediate the relationship between perceived system risk and resilience, and selfless misuse intention.

## **CHAPTER 2**

### **THEORETICAL BACKGROUND**

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; Pahnla et al. 2007), individuals may still tend to engage in inappropriate behaviors for other reasons. Therefore, in the IS security literature, multiple theories and concepts have been applied to explain individual rational behaviors in terms of information security. For example, based on the neutralization theory, individuals have been found to rationalize their violations of security policies by using several neutralization techniques (e.g., defense of necessity) (Siponen and Vance 2010). In addition, some studies have shown that a decision to engage in criminal behavior is a function of the subjective expectations of cost and benefit by the individual (Becker 1968; Cornish and Clarke 2014; Paternoster and Simpson 1996). Other studies have shown that individuals seem to be not motivated to comply with security policies. For instance, in one study (Stanton et al. 2005), it was suggested that employees may not be motivated to protect their organization's information and technology resources as required by the information security policy. In another study (Pahnla et al. 2007), based on the protection motivation theory (PMT) and deterrence theory, it was found that both the effects of coping appraisal (e.g., response efficacy, self-efficacy, and response cost), and sanctions were not significant regarding

employees' behavior towards IS security policy compliance. Furthermore, many studies have found that when employees experience difficulties in working around operational failures in a policy-compliant manner, they will engage in risky workarounds to complete their tasks (Ash et al. 2004; Halbesleben et al. 2008; Holden et al. 2013; Koppel et al. 2008). Although the growing interest and research efforts in studying individuals' rational behavior in terms of information security based on the rational choice theory (RCT) (McCarthy 2002), neutralization theory (Siponen and Vance 2010), protection motivation theory (PMT), deterrence theory (Pahnila et al. 2007), and workarounds (Debono et al. 2013; Koppel et al. 2008; Tucker and Hall 2013), some critical questions remain unanswered, especially under the context of disasters. The literature has investigated individual rational behaviors such as engaging in IS misuse, violations, workarounds, and complying with security policies under normal situations, on the other hand, it has neglected the context of disruptions and disasters. Since organizations have been facing various disruptions caused by natural disasters (e.g., hurricanes, earthquakes, floods, and tsunamis), there is a clear need for understanding the issues regarding individual rational behaviors in engaging in IS misuse in such situations. In the following subsections, we explain how the rational choice theory (RCT), neutralization theory, protection motivation theory (PMT), deterrence theory, and workarounds may not be directly applicable under the context of disasters. Then, we concentrate on the concept of bounded rationality, cost-benefit approach, and selfless misuse regarding individual behaviors, which are brought by the context of disasters.

### **Rational Choice Theory (RCT)**

According to the rational choice theory (RCT), individuals tend to behave rationally, and they determine how they will act by balancing the costs and benefits of their options. Basically, individuals have preferences for outcomes, so they perceive each outcome to be associated with a cost or a benefit depending on how much satisfaction the outcome will produce for them (McCarthy 2002). Hence, they shape their overall assessment of the costs and benefits of their course of action based on their perceptions of the potential outcomes associated with that course of action (Bulgurcu et al. 2010). In this case, from a rational-choice perspective, individuals frame security measures as interference with their job responsibilities and the practical accomplishment of their work based on their perspectives of

IS security in terms of costs and benefits (Dourish et al. 2004; Post and Kagan 2007), therefore they ignore policies and bypass security measures if that can improve their job performance and help them to do their work (Guo et al. 2011).

Despite the RCT has been shown to be useful in explaining behaviors, it is not exempt from criticism, especially under the context of disasters. In rational decision making, individuals' choices are harmonious with their preferences (McCarthy 2002). Basically, when individuals make a decision based on their assessment of costs and benefits, the decision should be consistent with their preferences in order to be rational (Bulgurcu et al. 2010). Otherwise, under the context of disasters, individuals experience extreme situations that can affect their rational decision-making process, and the way they act as they normally do under normal situations. Since disasters can increase pressure to act quickly, and place responders at risk (Kathleen Geale 2012), individuals will be forced to make quick decisions to behave. Hence, individuals may not be able to make optimal decisions that are consistent with their preferences due to time limitation and risks brought by the disaster context. In this case, since rationality is based on the consistency between individuals' choices and preferences (McCarthy 2002), the rational choice theory (RCT) may not be applicable under the context of disaster.

### **Neutralization Theory**

According to the neutralization theory, Siponen and Vance (2010) proposed a neutralization model that suggests that employees rationalize their violations of security policies by using several neutralization techniques (e.g., denial of responsibility, denial of injury, and the defense of necessity). Based on their findings, the neutralization techniques had a significant positive effect on employee intentions to violate IS security policies, and the effects of sanctions were not significant in the study. In addition, neutralization techniques have previously been successfully applied to explain rule-breaking behaviors (Pershing 2003) and predict corporate crime (Piquero et al. 2005). However, even though prior studies have shown that these neutralization techniques have been used successfully by individuals when rationalizing their violation behaviors, they may not be applied under the context of disaster. For example, under normal situations, individuals act normally and rationally when using these neutralization techniques to justify their actions (e.g., IS violations). But, in the context

of disaster, such lack of information (Amaratunga et al. 2009), risks, and pressure (Kathleen Geale 2012) can limit individuals' ability to act normally and use such technique to rationalize their behaviors. In addition, using neutralization techniques such as denial of responsibility (e.g., denying responsibility for actions), denial of injury (e.g., justifying actions by minimizing the harm they cause) (Sykes and Matza 1957), and defense of necessity (e.g., viewing actions as necessary) (Minor 1981) may not be strong motivations or reasons for individuals to misuse IS, especially during extreme situations. Individuals make poor decisions about disaster management due to psychological, organizational, and economic reasons (Michel-Kerjan and Slovic 2010), and they tend to act altruistically when experiencing natural disasters (i.e., giving, helping and sharing) (Li et al. 2013). Hence, misusing IS for them will be more likely their responsibility and beyond the neutralization techniques. Thus, under the context of disasters, the neutralization theory may not be applicable and good enough to explain individuals' IS misuse or violation behaviors.

### **Protection Motivation Theory (PMT)**

The protection motivation theory (PMT) is an explanatory theory that predicts individuals' intention to engage in protective actions (Anderson and Agarwal 2010). It originates from both the threat appraisal and the coping appraisal. Threat appraisal has been defined as individuals' assessment of the level of danger posed by a threatening event while the coping appraisal describes their assessment of their ability to cope with and avert the potential loss or damage arising from the threat (Woon et al. 2005). The PMT has been found useful in predicting individuals' behaviors related to computer security (Anderson and Agarwal 2010) and information systems security policy compliance (Ifinedo 2012). For instance, in a recent study (Pahnila et al. 2007), based on the protection motivation theory (PMT), it was found that the effect of coping appraisal (e.g., response efficacy, self-efficacy, and response cost) was not significant regarding employees' behavior towards IS security policy compliance. Despite the capability of the protection motivation theory (PMT) to explain individuals' intention to engage in protective actions (e.g., ISSP compliance), it does not explain why individuals break rules (e.g., IS misuse or violation). In general, protective actions seem to represent the opposite of IS misuse. In addition, since individuals make poor decisions (Michel-Kerjan and Slovic 2010), behave quickly due to being at risks (Kathleen

Geale 2012), and act altruistically (Li et al. 2013) during disaster situations, they may not consider engaging in protective actions. This is consistent with the study that suggests that employees may not be motivated to protect their organization's information and technology resources as required by the information security policy (Stanton et al. 2005). Hence, the protection motivation theory (PMT) may not be operational under both the context of disaster and IS misuse.

### **Deterrence Theory**

The deterrence theory has been applied in many studies to investigate the effects of organizational deterrent measures on individual behaviors. For instance, in one study (D'Arcy et al. 2009), an extended deterrence model was proposed to examine the effects of perceived severity and certainty of sanctions on IS misuse intention. It was found that the effect of perceived severity of sanctions on IS misuse intention was significant, on the other hand, the effect of perceived certainty of sanctions was not, which is contrary to what is expected in the deterrence theory. In another study (Siponen and Vance 2010), a neutralization model was proposed that suggests that employees' violations of security policies is not always best explained by fear of sanctions because employees use several neutralization techniques. Based on the findings, the effects of sanctions were not significant. Furthermore, based on the general deterrence theory, Pahnla et al. (2007) has examined the effects of sanctions on employees' intention to comply with IS security policies. However, the effects of sanctions were not significant as well in the study. The deterrence theory may help to explain why individuals comply with computer use or security rules (e.g., by not engaging in IS misuse), but it does not explain why individuals break these rules or engage in IS misuse. This is consistent with the studies mentioned earlier that have shown that the effects of deterrence are not conclusive. Therefore, since the deterrence theory is not applicable in explaining the reasons behind individuals' IS misuse under normal situations, it will not be operational in the context of disaster as well.



## Workarounds

Workarounds have been classified as hindrance (e.g., circumvent system procedures or process perceived to be too time consuming, onerous or difficult), harmless (e.g., do not significantly affect workflow), and essential (e.g., to complete the tasks at hand) (Burns et al. 2015; Ferneley and Sobreperéz 2006). These workarounds are compensative responses that aim to achieve a work goal that otherwise would have been blocked by operational failures (Halbesleben et al. 2008; Kobayashi et al. 2005). According to the literature, healthcare providers often engage in these workarounds when perceiving inconveniences or inefficiencies to meet the pressing needs of the situational context (Debono et al. 2013; Koppel et al. 2008; Tucker and Hall 2013). Basically, healthcare providers have a workaround culture in which employees work around operational failures to improve their organizational performance (Koppel et al. 2008). For instance, in a recent study (Burns et al. 2015), the role of contextual integrity was examined to understand workaround decisions in the healthcare sector. The purpose of the study was to analyze healthcare employees' willingness to engage in a series of electronic medical record (EMR) workaround scenarios. It was found that healthcare employees were less inclined to engage in workaround behaviors that violate patient privacy and do not directly impact patient care (e.g., sharing credentials and using a file transfer app to transfer unencrypted patient records). Otherwise, they were more inclined to engage in workaround behaviors that involve patient treatment and dealing with a system failure (e.g., delegating system use to other employees and using personal device to transfer patient files). Workarounds have been considered necessary to deliver care and not legally sanctioned (Debono et al. 2013), but they can lead to circumvent privacy safeguards built into systems and formalized routines (Murphy et al. 2014). This is consistent with many studies that have found that when employees experience difficulties in working around operational failures in a policy-compliant manner, they will engage in risky workarounds to complete their tasks (Ash et al. 2004; Halbesleben et al. 2008; Holden et al. 2013; Koppel et al. 2008). Even though the concept of workarounds has shown that individuals engage in IS misuse (e.g., risky workarounds), especially under the context of operational failures and patient care, individuals may engage in IS misuse for other reasons in different contexts. For example, under normal situations, employees rationalize their risky workaround behaviors based on specific conditions such as patient care and operational failures. Hence, they engage in

workaround behaviors that only involve patient care and operational failures, but not those workaround behaviors that violate patient privacy (e.g., sharing credentials or IS misuse) (Burns et al. 2015). However, under the context of disaster, employees do not act normally and rationally due to the extreme situations they experience such as lack of information (Amaratunga et al. 2009), risks, and pressure (Kathleen Geale 2012). Thus, their rationalization of their workaround behaviors will be affected and limited. In this case, since they act altruistically during disasters (Li et al. 2013), they may engage in workaround behaviors that even violate patient privacy (e.g., IS misuse) for sake of both patient care and business continuity. Hence, the concept of workarounds is limited in explaining the exact reasons behind individuals' IS misuse. This is due to its lack of considering the situational factors that can limit individuals' rationality under the context of disaster.

### **Bounded Rationality under Extreme Events**

Disasters bring unique situations that place individuals at risk and pressure them to act quickly. 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. Therefore, our understanding of the factors that motivate individuals to engage in IS misuse behavior under the context of disasters is still limited. According to Simon (1990), individuals' rationality can be limited by their cognitive ability and information availability. For example, 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). Additionally, the complexity of a situation may make it difficult for individuals to simplify the circumstances in order to make optimal decisions. Therefore, Simon (1972) argues that these limitations are the main reasons behind the bounded rationality in individuals' decision-making process. As a result, in an effort to compensate for these limitations, decision-makers 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). There have been several contexts which confine individuals' decision-making. 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). Due to these contexts, decision-

makers act within high levels of uncertainty (Simon 1996), which particularly gives them no choice between satisfactory and optimal solutions except accepting a “satisficing” solution (Bouraoui and Lizarralde 2013). This limited rationality could be more extreme in hospital context. Since disasters can reduce users’ accessibility to information, increase difficulties for them to communicate and collaborate with colleagues, increase pressure to act quickly, and highly likely place them at risk, they could become unable to find or process all the information about patients or the organization (i.e., cognitive limitations). These cognitive limitations could encourage them to act under the certain level of uncertainty.

### **Uncertainty from Disasters**

Uncertainty is defined as individuals’ perception of themselves as unable to predict something accurately (Milliken 1987). Uncertainty has been shown to come from lack of information, which makes it difficult for individuals to construct a plausible interpretation about situations. For example, individuals may be unable to precisely estimate the consequences of their current actions on the future (March 1994), such as if employees engage in selfless misuse will harm their organization in terms of information security or if they do not engage in selfless misuse will harm it in terms of patient care and business continuity. Hence, due to individuals’ inability to foresee the consequences of their current actions, this may lead them to construct an occasion for sensemaking during which they try to reduce their uncertainty (Weick 1995). Uncertainty about one’s perceptions, attitudes, feelings, and behaviors has a powerful motivational effect, therefore individuals who are uncertain about their identity are particularly motivated to reduce uncertainty (Van Lange et al. 2011).

In this study, uncertainty is defined as lack of confidence in individuals’ ability to predict particular outcomes (Penrod 2001). Our interests specifically lie in individuals’ sense of unpredictability about the safety of patients, safety of hospital, capability of HIS to recover, and their ability to perform the job under the context of disaster.

### **Cost-benefit Approach**

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). According to the rational choice theory (RCT), individuals tend to behave rationally, and they determine how they will act by balancing the costs and benefits of their options. Basically, individuals have preferences for outcomes, so they perceive each outcome to be associated with a cost or a benefit depending on how much satisfaction the outcome will produce for them (McCarthy 2002). Hence, they shape their overall assessment of the costs and benefits of their course of action based on their perceptions of the potential outcomes associated with that course of action (Bulgurcu et al. 2010). In rational decision making, individuals' choices are harmonious with their preferences (McCarthy 2002). Basically, when individuals make a decision based on their assessment of costs and benefits, the decision should be consistent with their preferences in order to be rational (Bulgurcu et al. 2010).

However, under the context of disasters, this cost-benefit approach is used differently than it is under normal situations. This is due to the high level of uncertainty from disasters, which can affect individuals' decision-making process by causing bounded rationality. Individuals are unable to foresee the consequences of their current actions under uncertainty, therefore they may engage in sensemaking for the sake of reducing their uncertainty (Weick 1995). Sensemaking is the complex cognitive process, which individuals engage in under complex and high-risk situations (Weick 1995). Thus, we argue that this complex cognitive process may cause employees to act based on a reasonable and limited cost-benefit analysis. Since intrinsic motivations can influence individual intentions regarding an activity (Davis et al. 1992), in this study, these costs and benefits may be considered as intrinsic motivations for employees' HIS use behavior since they would need rational reasons under the disaster context when they decide to selflessly misuse their HIS.

## CHAPTER 3

### LITERATURE REVIEW

#### **Perceived System Risk**

Employees perceive system risks based on their subjective expectations and assessments of the risks caused by damage or loss to information systems (Straub and Welke 1998), therefore they face feelings of discomfort or anxiety (Dowling and Staelin 1994), concern (Zaltman and Wallendorf 1983), uncertainty (Engel et al. 1986), and cognitive dissonance (Festinger 1957). Perceived risk increases the levels of expectation and pessimism regarding information systems' capabilities in supporting employees' jobs, which negatively influences individual performances, and then leads to employees' avoidance and ineffective use of the organization's information systems (Park et al. 2015). So in the context of disasters, this perception of system risks will be very high because disasters can reduce employees' sense of safety (Kroon and Overdijk 1993), highlight and amplify their personal insecurities and feelings of vulnerability (Wolfenstein 1957), and increase their stress levels, which in turn negatively affects the image of the organization's capabilities. Since fear to lose of all or a portion of the healthcare information system (HIS) functionality would quickly compromise 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), employees could increase their perception of system risks that eventually could impact their behavior (Heal and Kunreuther 2007), prevent their positive action (Jiang and Klein 1999), and negatively influence their performances (Park et al. 2015).

#### **System Resilience**

Resilience has been defined as the "system's ability to anticipate and respond to anomalous circumstances so as to maintain safe function, recover, and return to stable equilibrium (to the original operating state or to a different state)" (Sheridan 2008). In addition, resilience has been identified with three central features, which are systems' ability

to absorb or buffer disturbances and still maintain their core attributes, systems' ability to self-organize, and systems' capacity for learning and adaptation in the context of change (Berkes et al. 2008). Based on prior studies, resilience has been shown to help in the reduction of the consequences of negative events (Heal and Kunreuther 2007), therefore it is important in the context of disasters due to its capability to bounce back (Wildavsky 1988). Resilient infrastructures have been shown to enable organizations to maintain positive adjustment under challenging conditions (Sutcliffe and Vogus 2003) by reducing their vulnerabilities (Sheffi and Rice Jr 2005) and providing them with the means to target resource investments through integrating safety and productivity concerns (Nemeth et al. 2008).

So, in hospital context, lack of system resilience under disasters could be very extreme. For example, in hospital, disasters can reduce access to information (Amaratunga et al. 2009) and amplify personal insecurities and feelings of vulnerability (Wolfenstein 1957), therefore employees' stress levels and perceptions of system risk will increase (Park et al. 2015), which in turn negatively affect their feelings about the usage of the healthcare information system (HIS) and increase their intention to misuse it for the sake of delivery of health services and business continuity.

In fact, in the interview with the chief information officers of hospitals that were affected by the October 2006 snowstorm of western New York,

*“When the employees felt that the risk to the system was high, it impacted the perception of the usefulness of the systems and caused users to switch to manual systems much earlier [on receipt of the impending snowstorm warning—which later turned into an unanticipated disaster] and after the storm, they did not believe the IT department’s notifications that the disaster recovery process had been completed and they did not switch back to the HIS even though they were repeatedly reminded. This consequently had an impact on the efficiency of patient care and slowed patient care for days after the snowstorm.” (in Park et al., 2015, p. 319).*

We believe that increasing system resilience (the capabilities for rebounding quickly) will reduce the hospitals' vulnerabilities and improve their processes in ensuring the delivery of health services and business continuity. For instance, a study has explained how system resilience can play an important role in ensuring delivery of health services. It illustrates that

gaps in the continuity of care prove that healthcare information systems (HIS) are unable to respond with sufficient output to meet demand, therefore the ability of systems to respond to fill such gaps in care continuity indicates their resilience (Nemeth et al. 2008). Hence, we posit that a high level of system resilience in hospitals will reduce employees' perceptions of system risk, which will in turn affect their feelings (e.g., intrinsic benefits and intrinsic costs) about misusing the healthcare information system (HIS). In this study, we define system resilience as employees' beliefs regarding the capacity of the information systems to maintain and cope with damages or losses (Rose 2004).

### **Conceptualization of Selfless Misuse under Disaster Context**

In general, IS misuse refers to individuals' inappropriate behavior in using IS resources (Magklaras and Furnell 2001). This misuse behavior is quite varied that ranges from behaviors that are unethical and/or inappropriate to those that are illegal. IS misuse behaviors cover four areas: (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 (Park et al. 2015). Unauthorized access to computerized data has been reported as one of the most common types of breaches in organizations (Richardson 2007). In addition, 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, they are the ones employees may engage in when attempting to ensure delivery of health services and business continuity during disaster situations. Thus, we consider them as representative of typical IS misuse issues often encountered by organizations, which include accessibility, privacy, property, and accuracy (Mason 1986).

In disaster context, individuals' misuse behavior highly likely appears in different aspects from normal situations. The unexpectedness and urgency from disaster contexts may inevitably cause individuals to inappropriately use their IS resources to do their job. In this case, misusing IS resources to conduct their work is more likely to be their responsibility even though their behaviors should not be encouraged to do so. Since disasters can reduce users' accessibility to information, lead them to difficult communications and collaborations with

colleagues, increase pressure to act quickly, and highly likely place them at risk, they could become a cognitively limited state of mind to find or process all the information about patients or the organization. Even as a disaster situation triggers uncertainty for individuals to be irrational or limited rational thinking, it could be more difficult for them to decide whether they misuse the resources.

Especially, in hospital context, employees' decision to misuse seems to be extremely hard under the disaster context because they are under the thin line between patient care and following rules in using their resources such as HIS. Thus, when employees decide to misuse HIS under disaster context, they are more likely to do it not because of their own selfish purposes (e.g., satisfaction) but because of moral or ethical issues, such as ensuring the delivery of health services to patients and to continue their business. This different purpose of misuse in hospitals could result in the uniqueness of this study that HIS misuse reflects 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. Even though selfless misuse is considered unethical or illegal, it can be a moral 'right to do' due to the inevitability caused by uncertainty under disaster context. This is consistent with the study that has shown that individuals tend to act altruistically when experiencing natural disasters (i.e., giving, helping and sharing) (Li et al. 2013). For example, one may share passwords to ensure the delivery of health services and business continuity for the sake of helping others.



## CHAPTER 4

### MODEL DEVELOPMENT AND HYPOTHESES

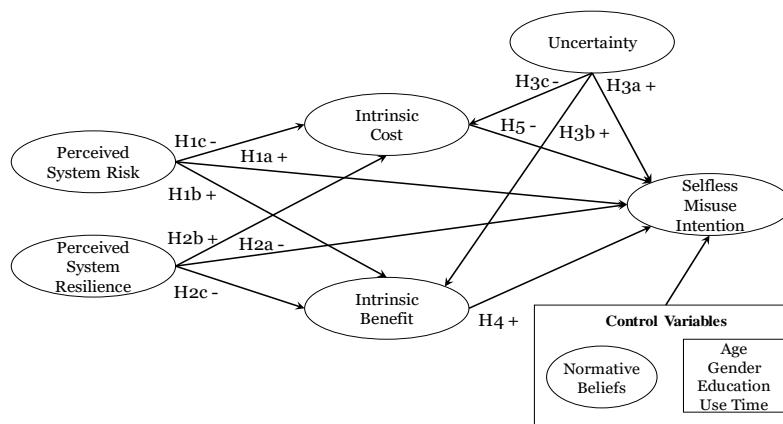


Figure 1. The Proposed Model

#### 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 selfless 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' selfless 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 selflessly misuse their HIS if doing so can help them to do their jobs, especially under extreme and urgent situations. Thus, we hypothesize:

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

A past study has found that there is an inverse relationship between perceived risk and perceived benefit of an activity, which can be determined through the strength of positive or negative affect that is associated with the activity (Alhakami and Slovic 1994). For instance, when perception of risk is high for an activity or technology, this would lead to more negative affect that would, in turn, decrease the perception of benefit of that activity or technology. The definition of "affect" was as specific quality of "goodness" or "badness" that can be experienced as a feeling state and demarcating a positive or negative quality of a stimulus (Slovic et al. 2004). In our study, we apply this approach and use intrinsic cost as specific quality of "negative feeling" and intrinsic benefit as specific quality of "positive feeling" that are associated with the usage of the healthcare information system (HIS). Disasters bring employees' perception of system risks, eventually it could lead high possibility of misusing HIS. Since HIS is a fundamental infrastructure that is strongly supporting social community, it should be continuously implemented to deliver health services and business continuity under the disaster situations. Based on the study that people have shown the altruistic tendency under extreme events (Li et al. 2013), hospital employees also would likely consider misusing HIS to be benefits for stakeholders (i.e., patients, hospital), even though it may be unethical or a violation of hospital policy. Thus, in hospitals under disaster situations, when employees perceive high system risks, they would also feel that this type of misuse would be a benefit to stakeholders. Thus, we hypothesize:

***Hypothesis 1b:*** *Perceived system risk increases employees' intrinsic benefit of selfless misuse under disaster context.*

***Hypothesis 1c:*** *Perceived system risk decreases employees' intrinsic cost of selfless misuse under disaster context.*

### **Perceived System Resilience**

The state of hospitals can be vulnerable if 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 (Dawes et al. 2004; Helsloot 2005; Junglas and Ives 2007; Pan et al. 2005). The 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, which would include business continuity, disaster recovery (Park et al. 2015), and IT systems configuration (Nemeth et al. 2008). Resilience has been shown to play an important role in the reduction of the consequences of negative events (Heal and Kunreuther 2007) due to its capability to bounce back (Wildavsky 1988) and reduce organizational vulnerabilities (Sheffi and Rice Jr 2005). 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. Thus, when HIS is capable of ensuring information availability, employees will be able to do their jobs, which can decrease their perceived system risk that would, in turn, lead to decrease their intrinsic cost and increase their intrinsic benefit about using the healthcare information system (HIS). As a result, this would in turn lead to increase the perceived benefits of HIS. This is consistent with a study that has shown that when perception of risk is low for an activity or technology, this would lead to more positive affect that would, in turn, increase the perception of benefit of that activity or technology (Slovic et al. 2004). 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 cost and decrease

their intrinsic benefit of selfless misuse intention. Thus, we hypothesize:

***Hypothesis 2a:*** *Perceived system resilience is negatively associated with employees' selfless misuse intention under disaster context.*

***Hypothesis 2b:*** *Perceived system resilience is positively associated with employees' intrinsic cost under disaster context.*

***Hypothesis 2c:*** *Perceived system resilience is negatively associated with employees' intrinsic benefit under disaster context.*

## **Uncertainty**

According to the Social Identity Theory (SIT), it posits that individuals tend to maintain high self-esteem by classifying themselves into social groups (Goldberg et al. 2010). In addition, prior studies have noted that reducing uncertainty in one's identity is a primary motive in social identification (Hogg 2008; Hogg and Abrams 1993; Smith et al. 2007). Since disasters can decrease the perceived self-competence and self-esteem of individuals (Wolfenstein 1957), individuals who are affected by them may experience negative expectations of their identity in the organization. This is due to their lack of confidence in their ability to predict particular outcomes under uncertainty (Penrod 2001). Hence, individuals who are uncertain about their identity are particularly motivated to reduce their uncertainty (Van Lange et al. 2011). As a result, in our study, we argue that employees' sense of unpredictability about the safety of patients, safety of hospital, capability of HIS to recover, and their ability to perform the job under the context of disaster could motivate them to act based on what enhances their identity. For example, employees may engage in selfless misuse to ensure patient care and business continuity, which in turn leads to enhance their self-esteem and self-competence. Thus, we posit that employees' uncertainty may lead to increase their intrinsic benefit, decrease their intrinsic cost, and increase their selfless misuse intention for the sake of meeting their identity needs.

***Hypothesis 3a:*** *Uncertainty is positively associated with employees' selfless misuse intention under disaster context.*

***Hypothesis 3b:*** *Uncertainty is positively associated with employees' intrinsic benefit under disaster context.*

***Hypothesis 3c:** Uncertainty is negatively associated with employees' intrinsic cost 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. In this study, we define intrinsic benefit as employees' positive feeling such as accomplishment, while intrinsic cost as employees' negative feeling such as stress (Bulgurcu et al. 2010). 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). In disaster situation, employees may attempt to do sense-making, which is the simplest way to find satisficing solutions that can help them to do their jobs while reducing their uncertainty. Therefore, they may simply act based on a limited evaluation of intrinsic cost and intrinsic benefit. Since Weick (2005) said, individuals tend to do sense-making in order to meet their general long-term goals, we argue that employees' intrinsic benefit may dominate their intrinsic cost for the purpose of meeting their goals (i.e., organizational commitment or altruism in the organization). This is consistent with the study that has shown how responsible officials have failed to take appropriate actions during pre-impact periods of possible disasters because of their fear about generating panic. The Weather Bureau and the Coast Guard, for instance, have announced an immediate evacuation of the ocean resort town, but city officials and the state police refused to order the evacuation because of their fear that such action might precipitate a panicky flight, even though they knew that the only two evacuation routes would become impossible if the hurricane heading for their low-lying area was as intense as predicted (Quarantelli 1975). Their decision was inappropriate, but they might have made it for the greater good. Thus, we believe that employees may act that way because of the importance of delivery of health services and business continuity that may lead to their organizational commitment or altruism in the organization. Thus, we hypothesize the following:

***Hypothesis 4:** Employees' intrinsic benefit is positively associated with their selfless misuse intention under disaster context.*

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; Pahlila et al. 2007). For instance, a recent study has examined the antecedents of IS misuse intention and found that perceived severity of sanctions can reduce IS misuse intention (D'Arcy et al. 2009). Sanctions are indeed useful, but they are not the only events that can lead to the formation of employees' beliefs about the cost of not adhering to the security-related rules and regulations (Siponen 2000). Prior studies have highlighted the importance of self-imposed punishment as an effective deterrent for corporate employees, especially in the form of embarrassment and shame. They have also argued that self-imposed punishment can discourage employees from committing corporate crimes, therefore they have suggested that self-imposed punishment can be a highly strong source of social control (Paternoster and Simpson 1993; Paternoster and Simpson 1996). In addition, research on deterrence has found positive evidence that shame is a self-imposed sanction that can function as a deterrent and decrease individuals' motivations to perform crimes (Nagin and Paternoster 1993). Furthermore, based on a recent study, intrinsic cost as a negative feeling such as stress has been found effective in increasing employees' overall expected unfavorable consequences for noncompliance with the information security policy (ISP) (Bulgurcu et al. 2010). Following this study, we believe that employees' intrinsic cost may decrease their motivations to act inappropriately or illegally in their decision-making process, which is due to their expected unfavorable consequences for noncompliance with ISP. Hence, this may lead to discourage them to misuse the healthcare information system (HIS). Thus, we hypothesize:

***Hypothesis 5:** Employees' intrinsic cost is negatively associated with their selfless misuse intention under disaster context.*

### **Control Variables**

Based on the theory of planned behavior, it suggests that the intention to perform various kinds of behaviors can be predicted with high accuracy from subjective norms (Ajzen 1991), therefore it postulates that behavior can be explained by normative beliefs as an antecedent of subjective norms. Normative beliefs are defined as employees' perceived social pressure about not misusing the HIS caused by behavioral expectations of such important

referent as colleagues (Ajzen 1991; Fishbein and Ajzen 1977). Hence, we add normative beliefs to our model as a control variable since it has been found effective in explaining behaviors. In addition, because the extant literature has shown that age and gender can predict various forms of IS misuse (D'Arcy et al. 2009; Leonard and Cronan 2001; Leonard et al. 2004), in this study, age and gender are included as control variables. The study seeks to assess the impact of perceived system risk, perceived system resilience, uncertainty, intrinsic cost, and intrinsic benefit on selfless misuse intention, which is beyond these known predictors. Therefore, we believe that including them as control variables are important to account for potential differences in selfless misuse intention among users. Finally, we include education and use time of the healthcare information system (HIS) as control variables as well.

## **CHAPTER 5**

### **RESEARCH METHODOLOGY**

We used the survey method to test the proposed model. We developed the initial survey instrument by identifying appropriate measurement scales that were adapted from the existing measures used in prior studies that were proven reliable and valid. Additionally, we developed new measures by closely following the definitions of the constructs in the study. Table 1 presents all of the constructs, along with the definitions, number of their measurement items, and sources. The survey questions are shown in Table A1 in Appendix A.

Data was collected by administering a web-based questionnaire survey. The pool of survey participants was obtained from multiple hospitals located across the United States. We asked the research company to contact participants who are employed by hospitals located in disastrous areas in the United States. In total, 307 surveys were completed and included in the data analysis. A summary of the demographic characteristics of respondents is provided in Table 2.

Table 1. Definitions and Sources of Measurement Items

Constructs	Definitions	Items (reference)
SR	Subjective expectations and assessments of the risks caused by the loss or disruption of HIS (Straub and Welke 1998).	4 items (Bulgurcu et al. 2010)
SRE	Beliefs regarding the capacity of the information systems to maintain and cope with damages or losses (Rose 2004).	4 items*
UNT	Lack of confidence in individuals' ability to predict particular outcomes (Penrod 2001).	2 items (Afifi et al. 2012) 2 items*
IB	Positive feeling such as accomplishment.	4 items (Bulgurcu et al. 2010)
IC	Negative feeling such as stress.	4 items (Bulgurcu et al. 2010)
NB	Perceived social pressure caused by behavioral expectations of such important referent as colleagues.	4 items (Ajzen 1991)
SM	Intention to misuse HIS to do good.	2 items (D'Arcy et al. 2009) 2



		items*
C.V.	Normative beliefs (Ajzen 1991), age, gender, education, HIS use time	
<p>Note: SR: Perceived System Risk, SRE: Perceived System Resilience, UNT: Uncertainty, IB: Intrinsic Benefit, IC: Intrinsic Cost, NB: Normative Beliefs, SM: Selfless Misuse Intention, C.V.: Control Variables, Items*: developed by authors</p>		

Table 2. Demographic Characteristics of Respondents

<b>Survey participants (<i>n</i> = 307)</b>			
<b>Gender</b>			
Male	44		14.4%
Female	261		85.6%
<b>Age</b>			
18-24	0		0.0%
25-34	5		1.6%
35-44	39		12.7%
45-54	65		21.2%
55 and over	198		64.5%
<b>Education</b>			
Less than High School	0		0.0%
High School / GED	20		6.5%
Some College	39		12.7%
2-year College Degree	65		21.2%
4-year College Degree	121		39.4%
Master's Degree	32		10.4%
Doctoral Degree	9		2.9%
Professional Degree (JD, MD)	21		6.8%
<b>Healthcare information system use time (years)</b>			
Range		1—20	
Mean		8.74	
Std. deviation		5.98	

## CHAPTER 6

### DATA ANALYSES AND RESULTS

#### Data Analysis

Partial least squares (PLS), as implemented in SmartPLS version 2.0.M3, was used for data analysis due to its capability to allow researchers to assess measurement model parameters and structural path coefficients simultaneously. Since this study was primarily intended for causal-predictive analysis, the PLS approach should be an appropriate statistical analysis tool 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).

#### Common Method Bias

To identify common method bias in our study, we conducted a full collinearity test. This comprehensive procedure is fully automated by the software WarpPLS, which can generate variance inflation factors (VIFs) for all the latent constructs in the model. If VIFs are greater than 3.3, this means that the model may be contaminated by common method bias. On the other hand, if VIFs are equal to or lower than 3.3, the model can be considered free of common method bias (Kock 2015). Based on the full collinearity test, our model is free of common method bias because all the VIFs are lower than 3.3 (see Table 3).

Table 3. Full Collinearity VIFs

SR	SRE	UNT	IB	IC	SM
1.334	1.05	1.34	1.28	1.3	1.257

#### Measurement Model

The measurement model for all measures in the PLS analysis was assessed by examining internal consistency, convergent validity, and discriminant validity (Barclay et al. 1995). Table 4 shows that all validity and reliability are good with the average variance

extracted (AVE), cronbach's alpha (CA), and composite reliability (CR). All of the factor loadings exceeded 0.70, indicating adequate reliability (see Table 5). In addition, the square root of the average variance extracted (AVE) of each construct was greater than its correlation with other constructs.

Table 4. Inter-construct Correlation

	CA	CR	AVE	SR	SRE	UNT	IB	IC	SM
SR	0.93	0.95	0.84	<b>0.91</b>					
SRE	0.94	0.96	0.85	0.06	<b>0.92</b>				
UNT	0.90	0.93	0.76	0.45	0.14	<b>0.87</b>			
IB	0.90	0.93	0.77	0.18	-0.01	0.14	<b>0.88</b>		
IC	0.93	0.95	0.83	-0.09	0.11	-0.12	-0.40	<b>0.91</b>	
SM	0.93	0.95	0.82	0.27	-0.03	0.27	0.31	-0.28	<b>0.91</b>
Note: SR: Perceived System Risk, SRE: Perceived System Resilience, UNT: Uncertainty, IB: Intrinsic Benefit, IC: Intrinsic Cost, NB: Normative Beliefs, SM: Selfless Misuse Intention.									

Table 5. Cross-Loadings

	SR	SRE	UNT	IB	IC	SM
<b>SR1</b>	<b>0.88</b>	0.02	0.46	0.16	-0.07	0.23
<b>SR2</b>	<b>0.91</b>	0.08	0.41	0.18	-0.07	0.27
<b>SR3</b>	<b>0.93</b>	0.04	0.39	0.16	-0.10	0.27
<b>SR4</b>	<b>0.93</b>	0.09	0.39	0.17	-0.10	0.23
<b>SRE1</b>	0.03	<b>0.91</b>	0.10	-0.01	0.10	-0.08
<b>SRE2</b>	0.03	<b>0.91</b>	0.11	0.00	0.06	-0.01
<b>SRE3</b>	0.09	<b>0.92</b>	0.15	0.01	0.06	0.01
<b>SRE4</b>	0.09	<b>0.93</b>	0.17	-0.03	0.13	-0.01
<b>UNT1</b>	0.36	0.14	<b>0.87</b>	0.14	-0.08	0.18
<b>UNT2</b>	0.38	0.15	<b>0.89</b>	0.13	-0.09	0.22
<b>UNT3</b>	0.43	0.19	<b>0.86</b>	0.12	-0.06	0.15
<b>UNT4</b>	0.41	0.06	<b>0.87</b>	0.10	-0.16	0.33
<b>IB1</b>	0.17	-0.01	0.12	<b>0.90</b>	-0.38	0.28
<b>IB2</b>	0.10	0.01	0.13	<b>0.78</b>	-0.31	0.25
<b>IB3</b>	0.22	-0.01	0.17	<b>0.92</b>	-0.33	0.25

<b>IB4</b>	0.15	-0.04	0.08	<b>0.91</b>	-0.37	0.30
<b>IC1</b>	-0.14	0.09	-0.13	-0.36	<b>0.90</b>	-0.24
<b>IC2</b>	-0.03	0.07	-0.06	-0.35	<b>0.87</b>	-0.24
<b>IC3</b>	-0.07	0.09	-0.11	-0.39	<b>0.94</b>	-0.28
<b>IC4</b>	-0.09	0.12	-0.13	-0.34	<b>0.92</b>	-0.26
<b>SM1</b>	0.23	0.03	0.24	0.28	-0.22	<b>0.90</b>
<b>SM2</b>	0.26	-0.01	0.26	0.26	-0.26	<b>0.90</b>
<b>SM3</b>	0.24	-0.05	0.24	0.28	-0.29	<b>0.93</b>
<b>SM4</b>	0.26	-0.09	0.25	0.29	-0.25	<b>0.90</b>

### Structural Model Testing

Figure 2 presents the path coefficients for the structural model. First, as we hypothesized in H1a, perceived system risk had a significant positive effect on selfless misuse intention ( $\beta = 0.146, p < 0.05$ ). The positive effect of perceived system risk (H1b) was also significant for the intrinsic benefit of selfless misuse ( $\beta = 0.150, p < 0.05$ ). The relationship between perceived system risk and intrinsic cost of selfless misuse (H1c) is not significant ( $\beta = -0.047$ ). Next, for hypothesis H2a, the effect of perceived system resilience on misuse intention is not significant ( $\beta = -0.043$ ). For H2b, perceived system resilience has a positive effect on intrinsic cost ( $\beta = 0.125, p < 0.05$ ). For H2c, the effect of perceived system resilience on intrinsic benefit is not significant ( $\beta = -0.034$ ).

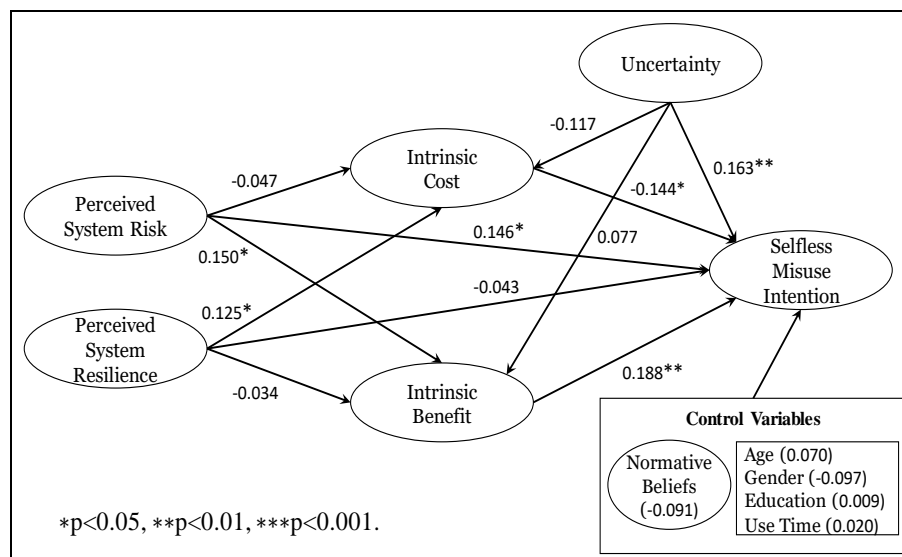


Figure 2. Results of Data Analysis

For hypothesis H3a, uncertainty has a significant positive effect on selfless misuse intention ( $\beta = 0.163, p < 0.01$ ), while on intrinsic benefit (H3b) and intrinsic cost (H3c), the one is not significant ( $\beta = 0.077, \beta = -0.117$ ).

For H4, intrinsic benefit has a positive effect on selfless misuse intention ( $\beta = 0.188, p < 0.01$ ). For H5, the effect of intrinsic cost is also significant for selfless misuse intention ( $\beta = -0.144, p < 0.05$ ).

### **Post-Hoc Analysis**

The purpose of the post-hoc analysis is to investigate the indirect effects of both perceived system risk and perceived system resilience on selfless misuse intention via two mediators, which are intrinsic cost and intrinsic benefit. To test for the significance of our indirect effects, we employed Sobel's mediation test (Sobel 1982). Due to the multiple mediators (intrinsic cost and intrinsic benefit), we investigated the effect of each respective mediator on the relationships in our model. While controlling for each mediator, this way allowed us to explore a specific mediated path, which provided information on the unique effect of each mediator (Bolger 1998). The results showed that perceived system risk significantly affects selfless misuse intention via only intrinsic benefit ( $\beta = 0.04, p < 0.05$ ), while the indirect effect of perceived system resilience on selfless misuse intention via only intrinsic cost was significant ( $\beta = -0.03, p < 0.05$ ).

## **CHAPTER 7**

### **DISCUSSION AND IMPLICATIONS**

#### **Discussion**

As hypothesized, we found that perceived system risk has a direct positive effect on selfless misuse intention. Besides that, we found that perceived system risk has a positive effect on intrinsic benefit as well. For perceived system resilience, we found that is not related to selfless misuse intention, while it has a significant positive effect on intrinsic cost.

One of findings says that uncertainty has a significant positive effect on selfless misuse intention, but not on intrinsic benefit and intrinsic cost. This suggests that employees do not consider the uncertainty as a factor for their cognitive judgement about how it would be cost or benefit for their decisions. Instead, it is considered as a factor to be minimized by making decision to misuse.

The post-hoc analysis shows interesting results about the differential effects of both mediators. That is, intrinsic benefit only mediates the effect of perceived system risk, while intrinsic cost only mediates the effect of perceived system resilience. A possible explanation is that employees highly likely consider intrinsic benefit of misusing HIS when being unable to perform their job due to system risks. On the other hand, they high likely consider intrinsic cost when being able to perform their job by relying on system resilience. This indicates that employees are more likely motivated to engage in selfless misuse based on the level of their perception of system risk as well as system resilience.

These findings eventually suggest that individuals in disaster contexts try to think rationally using rational tools such as cost-benefit approach, but there are still unexpected issues that they are not able to consider in their rational cognitive process. Obviously, uncertainty is the one of these issues and this brings them to the limited rational decision making that should be processed by cost-benefit approach. Specifically, our research shows that even though individuals act rationally based on the calculation of the cost-benefit analysis (Rational Choice Theory), their high level of uncertainty affects their decision-making but not this calculus process.

Furthermore, unlike a recent study (Bulgurcu et al. 2010) has shown that individuals tend to act rationally by increasing their benefit of compliance and increasing their cost of noncompliance with information security policy (ISP), this study shows that individuals tend to increase their intrinsic benefit and intrinsic cost based on their perception of system risk and resilience as factors affecting their decision-making process. Our results have demonstrated how individuals tend to engage in selfless misuse by increasing their intrinsic benefit even though it is against ISP, which is the opposite to the finding of the above-mentioned study as individuals increase their benefit of compliance with ISP. On the other hand, we showed that individuals increase their intrinsic cost of selfless misuse, especially when they are expecting unfavorable consequences for noncompliance with ISP.

Finally, based on the results, we found several insignificant relationships in the model. Interestingly, perceived system risk had an insignificant effect on intrinsic cost, whereas perceived system resilience had insignificant effects on both intrinsic benefit and selfless misuse intention. This indicates that employees are less likely influenced by their perception of system resilience when deciding to engage in selfless misuse. This is probably due to their high level of perception of system risk caused by disaster context. On the other hand, we also found that uncertainty had no significant effects on both intrinsic benefit and intrinsic cost. This finding suggests that employees are more likely influenced by their perception of system risk and resilience during their decision-making process. This could be due to the reasoning process employees engage in when deciding to selflessly misuse the HIS. For example, employees engage in the process of assessing their intrinsic benefit and cost of selfless misuse with a reason such as loss or disruption of the HIS. In this case, they assess them based on the level of their perception of system risk and resilience. Otherwise, if employees are under uncertainty, they immediately engage in selfless misuse without hesitation, which is why its significant direct effect on selfless misuse was very strong ( $\beta = 0.163, p < 0.01$ ).

### **Theoretical Contributions**

Our current study makes several significant contributions to the IS literature in terms of behavioral and organizational issues of information security. Based on our conceptual research model, we showed that perceived system risk and perceived system resilience play a role in affecting employees' decision-making process under the context of disaster. Specifically, we showed that employees' perceived system risk can impact their cost-benefit assessment as well as their decision-making by increasing their intrinsic benefit and selfless misuse intention. Besides that, we showed that perceived system resilience can enhance employees' cost-benefit assessment by increasing their intrinsic cost of selfless misuse.

Next, drawing on the concept of bounded rationality, since employees' cognitive limitations and lack of information under the context of disaster can lead them to act with a high level of uncertainty, we showed how uncertainty can directly lead them to engage in selfless misuse. In addition, we showed how employees tend to increase their intrinsic benefit of selfless misuse during their cost-benefit assessment for the purpose of meeting their goals as well. These results indicate that employees make poor decisions under disaster context due

to their high uncertainty and perceptions of system risk. Therefore, they engage directly in selfless misuse even though there is a cost associated with it. On the other hand, the results also indicate that employees are influenced by system resilience during their decision-making process, therefore they consider selfless misuse as a negative consequence leading to their high intrinsic cost.

Finally, while the extant literature has investigated individuals' IS misuse, violations, workarounds, and complying with security policies, this study is the first to investigate employees' selfless misuse, especially in the context of healthcare. Current theories, concepts, and models may not be operational under the context of selfless misuse because this concept is brought by the context of disaster. Our study demonstrates that employees tend to act altruistically under the context of disaster, especially in hospitals, therefore their misuse is considered both inappropriate and beneficial. As a result, selfless misuse may not be applicable in the existing models, which is due to its conceptualization as misuse with a strong intention to do good.

### **Practical Implications**

The study offers important practical implications for HIS security management practice. First, our results indicate that employees act poorly under extreme events, which is due to their high uncertainty and perception of system risk. Therefore, they tend to selflessly misuse HIS for the sake of delivery of health services and business continuity. When implementing a security policy, HIS security management should address how the enforcement of security policies can ensure a proper functionality of the healthcare information system, delivery of health services, and business continuity. This is consistent with the interview with the chief information officer of a hospital that was affected by the October 2006 snowstorm of western New York, "Having strong security processes may not help or may even hinder access to data during disaster situations. However, having a strong security posture would make people realize the hospital has good processes in managing the system at the data center and clinical levels for business continuity." (Park et al., 2015, p. 319).

Second, the findings of the present study raise some serious questions about the practical effectiveness of deterrent measures in reducing employees' inappropriate behavior.



If employees are cognitively limited and trying to ensure delivery of health services and business continuity for the greater good, prohibiting certain means of using HIS (e.g., misuse intention) will be problematic. Thus, it is important for HIS security management to provide alternative means that can help employees make the right decisions when performing their job, especially under extreme events. Such alternative means would be more useful for employees and thus would reduce their selfless misuse intention.

Third, this study indicates that employees' perception of system risks, uncertainty, and intrinsic benefit have a significant influence on their selfless misuse intention. This suggests that HIS security management should shift the way they train and educate employees. The HIS security management usually provides sufficient training and education to make employees aware of potential security risks, but that may not be sufficient since security risks may be too vague for employees. More importantly, security training and education should enable employees to have a good understanding of how the organization is capable of managing the healthcare information system for business continuity as well as make them realize that HIS misuse will affect the business performance of the organization.

Finally, hospitals should ensure the functionality of the healthcare information system (HIS) and access to information by increasing the ability of systems to adapt to and recover quickly from unexpected disruptions, which would include business continuity, disaster recovery, and IT systems configuration. Our results indicate that perceived system resilience can play an impotent role in discouraging employees to selflessly misuse their HIS.

## **CHAPTER 8**

### **LIMITATIONS, FUTURE RESEARCH, AND CONCLUSIONS**

Certain limitations of this study should be considered in interpreting our results. First, this study used specific IS misuse behaviors, therefore a limitation of this is that these IS misuse behaviors do not include every possible type of security violation. Thus, future

research should include more types of IS misuse behaviors to further test the proposed selfless misuse model. Second, we limited the concept of selfless misuse, which is defined as “Intention to misuse HIS to do good”, to the context of healthcare. Future research should examine selfless misuse in other different organizations under the context of disaster. A third limitation is that the study used selfless misuse intention instead of actual behaviors. Although intention is supported by the literature as a predictor of actual behavior, individuals may not behave as they have indicated. Hence, to add additional credibility to our model, future research should reexamine the model in a context where actual selfless misuse can be measured. A last limitation is that the study collected data from hospitals that are only located in disastrous areas. Future research should reexamine the model in a normal context where selfless misuse intention can be measured under normal situations.

Overall, the research profiled in this paper would contribute to understanding how hospital employees would misuse their information systems under disaster contexts. The results would call attention to how risk and resilience influence employees’ decision-making process and misuse intention. We hope that this study serves as encouragement for future research endeavors.

## REFERENCES

- Afifi, W. A., Felix, E. D., and Afifi, T. D. 2012. "The Impact of Uncertainty and Communal Coping on Mental Health Following Natural Disasters," *Anxiety, Stress & Coping* (25:3), pp. 329-347.
- Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational behavior and human decision processes* (50:2), pp. 179-211.
- Alhakami, A. S., and Slovic, P. 1994. "A Psychological Study of the Inverse Relationship between Perceived Risk and Perceived Benefit," *Risk analysis* (14:6), pp. 1085-1096.
- 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.
- Anderson, C. L., and Agarwal, R. 2010. "Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS quarterly* (34:3), pp. 613-643.
- Ash, J. S., Berg, M., and Coiera, E. 2004. "Some Unintended Consequences of Information Technology in Health Care: The Nature of Patient Care Information System-Related Errors," *Journal of the American Medical Informatics Association* (11:2), pp. 104-112.

- 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.
- Berkes, F., Colding, J., and Folke, C. 2008. *Navigating Social-Ecological Systems: Building Resilience for Complexity and Change*. Cambridge University Press.
- Bolger, N. 1998. "Data Analysis in Social Psychology," *Handbook of social psychology* (1), pp. 233-265.
- Bouraoui, D., and Lizarralde, G. 2013. "Centralized Decision Making, Users' Participation and Satisfaction in Post-Disaster Reconstruction: The Case of Tunisia," *International Journal of Disaster Resilience in the Built Environment* (4:2), pp. 145-167.
- 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.
- Burns, A., Young, J., Roberts, T. L., Courtney, J. F., and Ellis, T. S. 2015. "Exploring the Role of Contextual Integrity in Electronic Medical Record (Emr) System Workaround Decisions: An Information Security and Privacy Perspective," *AIS Transactions on Human-Computer Interaction* (7:3), pp. 142-165.
- 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.
- Cornish, D., and Clarke, R. 1986. "The Reasoning Criminal: Rational Choice Perspectives on Offending Springer-Verlag, New York," *NY Google Scholar*.
- 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.
- Davis, F. D., Bagozzi, R. P., and Warshaw, P. R. 1992. "Extrinsic and Intrinsic Motivation to Use Computers in the Workplace," *Journal of applied social psychology* (22:14), pp. 1111-1132.
- Dawes, S. S., Cresswell, A. M., and Cahan, B. B. 2004. "Learning from Crisis: Lessons in Human and Information Infrastructure from the World Trade Center Response," *Social Science Computer Review* (22:1), pp. 52-66.
- Debono, D. S., Greenfield, D., Travaglia, J. F., Long, J. C., Black, D., Johnson, J., and Braithwaite, J. 2013. "Nurses' Workarounds in Acute Healthcare Settings: A Scoping Review," *BMC health services research* (13:1), p. 175.
- Dourish, P., Grinter, R. E., De La Flor, J. D., and Joseph, M. 2004. "Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem," *Personal and Ubiquitous Computing* (8:6), pp. 391-401.
- Dowling, G. R., and Staelin, R. 1994. "A Model of Perceived Risk and Intended Risk-Handling Activity," *Journal of consumer research* (21:1), pp. 119-134.
- Engel, J., Blackwell, R., and Miniard, P. 1986. "Social Influence," in *Consumer Behavior*. CBS College Publishing New York, pp. 305-326.

- Ernst, Y. L., and Young, X. 2002. "Global Information Security Survey," *UK: Presentation Services*).
- Ferneley, E. H., and Sobreperéz, P. 2006. "Resist, Comply or Workaround? An Examination of Different Facets of User Engagement with Information Systems," *European Journal of Information Systems* (15:4), pp. 345-356.
- Festinger, L. 1957. "A Theory of Cognitive Dissonance: Stanford Univ Pr." sity Press, Stanford.
- Fishbein, M., and Ajzen, I. 1977. "Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research,").
- Goldberg, C. B., Riordan, C., and Schaffer, B. S. 2010. "Does Social Identity Theory Underlie Relational Demography? A Test of the Moderating Effects of Uncertainty Reduction and Status Enhancement on Similarity Effects," *Human Relations* (63:7), pp. 903-926.
- Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Richardson, R. 2005. "2005 Csi/Fbi Computer Crime and Security Survey," *Computer Security Journal* (21:3), p. 1.
- Guo, K. H., Yuan, Y., Archer, N. P., and Connelly, C. E. 2011. "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model," *Journal of Management Information Systems* (28:2), pp. 203-236.
- Halbesleben, J. R., Wakefield, D. S., and Wakefield, B. J. 2008. "Work-Arounds in Health Care Settings: Literature Review and Research Agenda," *Health care management review* (33:1), pp. 2-12.
- 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.
- Hogg, M. A. 2008. "Personality, Individuality, and Social Identity," *Personality and social behavior*), pp. 177-196.
- Hogg, M. A., and Abrams, D. 1993. "Towards a Single-Process Uncertainty-Reduction Model of Social Motivation in Groups,").
- Holden, R. J., Rivera-Rodriguez, A. J., Faye, H., Scanlon, M. C., and Karsh, B.-T. 2013. "Automation and Adaptation: Nurses' Problem-Solving Behavior Following the Implementation of Bar-Coded Medication Administration Technology," *Cognition, technology & work* (15:3), pp. 283-296.
- 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.
- Ifinedo, P. 2012. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," *Computers & Security* (31:1), pp. 83-95.
- Jiang, J. J., and Klein, G. 1999. "Risks to Different Aspects of System Success," *Information & Management* (36:5), pp. 263-272.
- 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.
- Kobayashi, M., Fussell, S. R., Xiao, Y., and Seagull, F. J. 2005. "Work Coordination, Workflow, and Workarounds in a Medical Context," *CHI'05 Extended Abstracts on Human Factors in Computing Systems*: ACM, pp. 1561-1564.
- Kock, N. 2015. "Common Method Bias in Pls-Sem: A Full Collinearity Assessment Approach," *International Journal of e-Collaboration (IJeC)* (11:4), pp. 1-10.
- Koppel, R., Wetterneck, T., Telles, J. L., and Karsh, B.-T. 2008. "Workarounds to Barcode Medication Administration Systems: Their Occurrences, Causes, and Threats to Patient Safety," *Journal of the American Medical Informatics Association* (15:4), pp. 408-423.
- Kroon, M. B., and Overdijk, W. I. 1993. "Psychosocial Care and Shelter Following the Bijlmermeer Air Disaster," *CRISIS-TORONTO*- (14), pp. 117-117.
- Leonard, L. N., and Cronan, T. P. 2001. "Illegal, Inappropriate, and Unethical Behavior in an Information Technology Context: A Study to Explain Influences," *Journal of the Association for Information Systems* (1:1), p. 12.
- Leonard, L. N., Cronan, T. P., and Kreie, J. 2004. "What Influences It Ethical Behavior Intentions—Planned Behavior, Reasoned Action, Perceived Importance, or Individual Characteristics?," *Information & Management* (42:1), pp. 143-158.
- 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.
- March, J. G. 1994. *Primer on Decision Making: How Decisions Happen*. Simon and Schuster.
- Mason, R. O. 1986. "Four Ethical Issues of the Information Age," *Mis Quarterly*, pp. 5-12.
- McCarthy, B. 2002. "New Economics of Sociological Criminology," *Annual Review of Sociology*, pp. 417-442.
- Michel-Kerjan, E., and Slovic, P. 2010. *The Irrational Economist: Making Decisions in a Dangerous World*. PublicAffairs.
- Milliken, F. J. 1987. "Three Types of Perceived Uncertainty About the Environment: State, Effect, and Response Uncertainty," *Academy of Management review* (12:1), pp. 133-143.
- Minor, W. W. 1981. "Techniques of Neutralization: A Reconceptualization and Empirical Examination," *Journal of Research in Crime and Delinquency* (18:2), pp. 295-318.
- Murphy, A. R., Reddy, M. C., and Xu, H. 2014. "Privacy Practices in Collaborative Environments: A Study of Emergency Department Staff," *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*: ACM, pp. 269-282.
- Nagin, D. S., and Paternoster, R. 1993. "Enduring Individual Differences and Rational Choice Theories of Crime," *Law and Society Review*, pp. 467-496.

- 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.
- Paternoster, R., and Simpson, S. 1993. "A Rational Choice Theory of Corporate Crime," *Routine activity and rational choice: Advances in criminological theory* (5), pp. 37-58.
- 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.
- Penrod, J. 2001. "Refinement of the Concept of Uncertainty," *Journal of Advanced Nursing* (34:2), pp. 238-245.
- Pershing, J. L. 2003. "To Snitch or Not to Snitch? Applying the Concept of Neutralization Techniques to the Enforcement of Occupational Misconduct," *Sociological Perspectives* (46:2), pp. 149-178.
- Piquero, N. L., Tibbetts, S. G., and Blankenship, M. B. 2005. "Examining the Role of Differential Association and Techniques of Neutralization in Explaining Corporate Crime,").
- Post, G. V., and Kagan, A. 2007. "Evaluating Information Security Tradeoffs: Restricting Access Can Interfere with User Tasks," *Computers & Security* (26:3), pp. 229-237.
- Quarantelli, E. L. 1975. "Panic Behavior: Some Empirical Observations,").
- 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.
- Sheffi, Y., and Rice Jr, J. B. 2005. "A Supply Chain View of the Resilient Enterprise," *MIT Sloan management review* (47:1), p. 41.
- Sheridan, T. B. 2008. "Risk, Human Error, and System Resilience: Fundamental Ideas," *Human Factors: The Journal of the Human Factors and Ergonomics Society* (50:3), pp. 418-426.
- Simon, H. A. 1972. "Theories of Bounded Rationality," *Decision and organization* (1:1), pp. 161-176.
- Simon, H. A. 1990. "Bounded Rationality," in *Utility and Probability*. Springer, pp. 15-18.
- 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.
- Siponen, M. T. 2000. "A Conceptual Foundation for Organizational Information Security Awareness," *Information Management & Computer Security* (8:1), pp. 31-41.

- Slovic, P., Finucane, M. L., Peters, E., and MacGregor, D. G. 2004. "Risk as Analysis and Risk as Feelings: Some Thoughts About Affect, Reason, Risk, and Rationality," *Risk analysis* (24:2), pp. 311-322.
- Smith, J. R., Hogg, M. A., Martin, R., and Terry, D. J. 2007. "Uncertainty and the Influence of Group Norms in the Attitude–Behaviour Relationship," *British Journal of Social Psychology* (46:4), pp. 769-792.
- Sobel, M. E. 1982. "Asymptotic Confidence Intervals for Indirect Effects in Structural Equation Models," *Sociological methodology* (13), pp. 290-312.
- Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J. 2005. "Analysis of End User Security Behaviors," *Computers & Security* (24:2), pp. 124-133.
- Straub, D. W., and Welke, R. J. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS quarterly*, pp. 441-469.
- Sutcliffe, K. M., and Vogus, T. J. 2003. "Organizing for Resilience," *Positive organizational scholarship: Foundations of a new discipline* (94), p. 110.
- Sykes, G. M., and Matza, D. 1957. "Techniques of Neutralization: A Theory of Delinquency," *American sociological review* (22:6), pp. 664-670.
- Tucker, A. L., and Hall, M. 2013. *Work Design Drivers of Organizational Learning About Operational Failures: A Laboratory Experiment on Medication Administration*. Harvard Business School.
- Van Lange, P. A., Kruglanski, A. W., and Higgins, E. T. 2011. *Handbook of Theories of Social Psychology: Volume Two*. SAGE publications.
- Weick, K. E. 1995. *Sensemaking in Organizations*. Sage.
- Wildavsky, A. B. 1988. *Searching for Safety*. Transaction publishers.
- Wolfenstein, M. 1957. *Disaster: A Psychological Essay*. Free Press and Falcon's Wing Press.
- Woon, I., Tan, G.-W., and Low, R. 2005. "A Protection Motivation Theory Approach to Home Wireless Security," *ICIS 2005 proceedings*, p. 31.
- Zaltman, G., and Wallendorf, M. 1983. "Consumer Behaviour." Wiley, New York.

## APPENDICES

### APPENDIX A

Table A1. Survey Questions

Constructs	Items	Scale
------------	-------	-------

Uncertainty	<p>Due to the natural disaster situation, I was uncertain about_____.</p> <ol style="list-style-type: none"> <li>1. the safety of patients.</li> <li>2. the safety of the hospital.</li> <li>3. the capability of the healthcare information system (HIS) to recover.</li> <li>4. how to perform my job.</li> </ol>	<p>1 = Strongly disagree 7 = Strongly agree</p>
Perceived System Risk	<p>Since the natural disaster occurred in the area, the loss or disruption of the healthcare information system_____.</p> <ol style="list-style-type: none"> <li>1. held me back from doing my actual work.</li> <li>2. slowed my response time to my colleagues, patients, and managers.</li> <li>3. hindered my productivity at work.</li> <li>4. impeded my efficiency at work.</li> </ol>	<p>1 = Strongly disagree 7 = Strongly agree</p>
Intrinsic Benefit	<p>Due to the loss or disruption of the healthcare information system, performing my job by_____.</p> <ol style="list-style-type: none"> <li>1. sharing passwords to do good makes me feel accomplished.</li> <li>2. accessing restricted information to deliver health services makes me feel accomplished.</li> <li>3. disclosing unauthorized confidential information to</li> </ol>	<p>1 = Completely disagree 7 = Completely agree</p>



ensure patient care makes me feel accomplished.

4. using email inappropriately to continue business makes me feel accomplished.

#### Intrinsic Cost

Due to the loss or disruption of the healthcare information system, performing my job by\_\_\_\_\_.

1 = Completely disagree

7 = Completely agree

1. sharing passwords to do good makes me feel stressed.
2. accessing restricted information to deliver health services makes me feel stressed.
3. disclosing unauthorized confidential information to ensure patient care makes me feel stressed.
4. using email inappropriately to continue business makes me feel stressed.

#### Perceived System Resilience

During the natural disaster situation, the healthcare information system was able to adapt to and recover quickly from disruptions, which\_\_\_\_\_.

1 = Strongly disagree

7 = Strongly agree

1. improved my ability to do my actual work.
2. enhanced my response time to my colleagues, patients, and managers.

	<ol style="list-style-type: none"> <li>3. increased my productivity at work.</li> <li>4. increased my efficiency at work.</li> </ol>	
Normative Beliefs	<p>During the natural disaster situation, my colleagues think that I should not_____.</p> <ol style="list-style-type: none"> <li>1. share passwords to do good.</li> <li>2. access restricted information to deliver health services.</li> <li>3. disclose unauthorized confidential information to ensure patient care.</li> <li>4. use email inappropriately to continue business.</li> </ol>	<p>1 = Completely disagree 7 = Completely agree</p>
Selfless Misuse Intention	<p>During the natural disaster situation, I intend to_____.</p> <ol style="list-style-type: none"> <li>1. share passwords to do good.</li> <li>2. access restricted information to deliver health services.</li> <li>3. disclose unauthorized confidential information to ensure patient care.</li> <li>4. use email inappropriately to continue business.</li> </ol>	<p>1 = Strongly disagree 7 = Strongly agree</p>

---