Abstract

Resilience has been studied extensively in humans but less attention has been paid to organizational resilience in hospital organizations. This research aims to offer solutions for effective management of extreme events in hospitals by investigating the antecedents of healthcare workers’ perceptions of organizational resilience. The theory of organizational resilience was used to examine the role of information privacy, information security, information access, leadership during emergencies, employee empowerment, and emergency training. A total of 402 survey responses were analyzed using Partial Least Squares regression. This is a research in progress.

Keywords: Business continuity, Resilience, Crisis management, Crisis response, Disaster Management, Emergency response

Introduction

When extreme events occur, they cause immediate catastrophic effects on nearly all aspects of an organization’s operations. Organizations can be viewed as complex systems composed of several interconnected components that work together to produce goods and services. In the context of healthcare organizations, an unplanned extreme event has the potential to disrupt all hospital operations, thereby threatening patient safety. As an example, an unplanned Electronic Medical Record (EMR) system outage may introduce patient safety risks due to limited access to patients’ medical information, resource shortages, cancellation of medical procedures, prolonged suffering due to delays and increased patient
wait time, etc. While extreme events are inevitable, hospitals must strive to sustain the continuity of medical services by developing strategies for minimizing the impact of the extreme events. One such strategy is increasing the hospital’s level of resilience to ensure continued delivery of high quality patient care following an extreme event.

The objective of this research in progress is to investigate the antecedents of healthcare workers’ perceptions of resilience in hospitals. Resilience is defined as the perception of a hospital’s ability to bounce back after an extreme event (Tugade & Fredrickson, 2004). Here, ‘bounce back’ reflects the hospital’s adaptive capacity, which is demonstrated by the ability to sustain continuity of critical medical services after an extreme event. The term extreme event is used to refer to an unplanned incident that disrupts the normal functioning of a hospital. The extreme event studied is an unplanned EMR outage lasting 24 hours. An EMR outage pertains to a period of time during which EMR systems are not available to the hospital staff. This research contributes to the existing IS literature by investigating the IS factors that influence resilience in hospital organizations. The research question that guides this study is as follows; what are the critical factors that influence healthcare workers’ perceptions of a hospital’s level of resilience after an extreme event? This question is answered using the theory of organizational resilience (Vogus & Sutcliffe, 2007).

The motivation for this research in progress is the evidenced lack of preparation for organizations to respond to extreme events, a lack of theoretical investigation of the Information Systems (IS) factors that facilitate resilience and overall, the limited research addressing these problems. Luftmann and Kempaiah (2008) found that a critical issue facing Information Technology (IT) executives was managing changes in the workplace, continuity planning, and disaster recovery. Later reports showed that technologies for business continuity planning and disaster recovery were ranked in the top five list of importance (Luftman & Ben-Zvi, 2010). These findings show the persistence of issues relating to disaster recovery and the need for addressing such issues. Elsewhere, Lurie, Manolio, Patterson, Collins, and Frieden (2013) recently noted that several factors exist that threaten the continuity of services during and following an extreme event. Other researchers have also pinpointed specific hindrances to achieving resilience, such as a lack of understanding of the parameters within an organization’s environment (McManus, Seville, Vargo, & Brunsdon, 2008). Despite these observations, limited attempts have been made to address these gaps in the literature.

The rest of the paper is organized as follows. The following section discusses the theoretical foundation and hypotheses development. This is followed by the methodology. Lastly, the findings and a discussion of the research implications are presented. This is a research in progress and as such, the results presented are preliminary and additional analysis is still underway.

Theoretical Background and Hypothesis Development

The theoretical lens for this work is organizational resilience theory, which describes the process of how organizations achieve desirable outcomes when faced with disturbances (Vogus & Sutcliffe, 2007). Organizational resilience theory puts emphasis on the organization as a system; all elements within the organization’s environment such as people, processes, and technology contribute to the organization’s overall performance. The focus is on the key organizational and individual attributes of an organization that contribute to resilience (Cameron & Dutton, 2003). Organizational resilience theory stems from the theory of resilience which describes an organization’s adaptive capabilities (Christianson, Sutcliffe, Miller, & Iwashyna, 2011; Vogus & Sutcliffe, 2007). In the organizational resilience context, the theory of resilience defines the ability of the organization to either maintain stability by absorbing change or adapt and ‘evolve’ based on the requirements of the environment (Folke, 2006). This suggests that elements within the organization’s environment contribute to the organization’s level of resilience. Because of the interrelatedness of elements within an organization’s environment, organizational resilience theory offers a mechanism to understand the organization’s ability to effectively respond to turbulence (Burnard & Bhamra, 2011). Earlier research has identified four categories of elements essential for achieving resilience, namely, leadership, employee empowerment, information services, and knowledge acquisition (McManus et al., 2008). Based on McManus et al. (2008)’s work, this research focuses on the following factors: leadership during emergencies, employee empowerment, emergency training, information access, information security, and information privacy. Here, the variables that relate to information services in this study are information privacy, information security, and information access. The variable relating to
knowledge acquisition is emergency training. The theoretical contribution of this work is the addition of two IS constructs to the organization resilience theory: information security and information privacy. As of the writing of this paper, this is the first study to investigate these constructs in the context of extreme events and organizational resilience.

In the following paragraphs, the hypotheses for the antecedents of healthcare workers’ perceptions of organizational resilience in hospitals are discussed.

**Information Privacy**

Information privacy pertains to the preservation of the privacy of information resources. The construct of information privacy is used in this research to refer to the effectiveness of information privacy controls. There are federal regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), which requires organizations to protect the privacy of patients’ medical records at all times. HIPAA requires organizations to have proper technical and physical controls in place for ensuring proper privacy of information (Health Insurance Portability and Accountability Act, 2003). Individuals handling patient information, such as healthcare workers, must also comply with HIPAA regulations as well. Ineffectiveness of technical privacy controls may therefore increase the burden of securing information for the healthcare workers by requiring them to manually complete privacy-preserving tasks. For instance, if the equipment responsible for shredding or disposing of sensitive information is not functional, staff is still required to dispose of the material in a secure way. Manual disposal of sensitive information may involve tearing the papers into tiny pieces; a process that may be tedious, time consuming, and prone to errors. On the contrary, effective privacy controls after an extreme event would reduce the amount of manual privacy preserving tasks for healthcare workers, which could increase the likelihood of the hospital’s ability to bounce back quickly. This leads to the following hypothesis:

Hypothesis 1: The effectiveness of information privacy controls will have a positive effect on healthcare workers’ perceptions of resilience in hospitals.

**Information Security**

Information security pertains to the protection of information resources from unauthorized use and access. In this research, we use information security to refer to the effectiveness of information security controls in terms of two aspects: the protection of information from internal and external threats, and the security policies relating to information sharing and access. An organization must have security safeguards for detecting both internal and external threats, and also protecting sensitive information from such threats. The second aspect of security deals with policies, which are often developed to ensure that employees comply with the established security rules, regulations, and guidelines when accessing and sharing sensitive information. In the aftermath of an extreme event, optimal security of patients’ medical information must be sustained to limit the possibility of security breaches, which would further strain the hospital’s resources. A security breach during the aftermath of an extreme event could cause delays due to the diversion of human resources from patient services to addressing the security breach. HIPAA requires organizations to secure electronic health records by putting the proper safeguards in place (Health Insurance Portability and Accountability Act, 2003); failure to provide adequate security measures may increase the workload of the hospital staff, consequently increasing the likelihood of negative perceptions regarding the hospital’s level of resilience. This leads to the following hypothesis:

Hypothesis 2: The effectiveness of information security controls will have a positive effect on healthcare workers’ perceptions of resilience in hospitals.

**Information Access**

Information access relates to the timely access of patient medical information by hospital workers. Access to timely and factual information during response activities improves an individual’s ability to make effective response decisions, and also increases the organization’s capacity to adapt to the extreme event (Comfort, Ko, & Zagorecki, 2004; Federal Emergency Management Agency, 2012). In the case of hospitals, hospital employees need timely access to patients’ records, treatment information, laboratory
Perceptions of Resilience after an Extreme Event

results, and other necessary information to enable continued provision of healthcare services, consequently enhancing the organization’s level of resilience. Based on this, we hypothesize the following.

Hypothesis 3: Access to information after an extreme event will have a positive effect on healthcare workers’ perceptions of resilience in hospitals.

**Leadership during emergencies**

This variable pertains to the perceived effectiveness of leadership during emergencies. When unplanned incidents occur, they interrupt normal operations thereby creating a unique set of challenges that if not properly managed, could interfere with the recovery and continuity of services. Leadership support during extreme events is essential in assisting individuals manage challenges and cope with the unstable circumstances associated with the event (VanDevanter, Kovner, Raveis, McCollum, & Keller, 2014). As healthcare workers tend to patients by continuing to provide patient care, it is likely that problems related to the extreme event may come up; it is therefore the responsibility of the leaders to effectively manage the event by resolving such problems as well as manage all other activities related to the extreme event (Waugh & Streib, 2006). In addition, perceptions of effective leadership have been shown to enhance subordinate commitment to excellence, increased level of participation, and commitment to quality performance (West et al., 2003). This prior research supports the hypothesis that when individuals perceive leadership to be effective, they are more likely to engage in positive performance behavior, consequently improving the organization’s level of resilience.

Hypothesis 4: The perceived effectiveness of leadership after the extreme event will have a positive effect on healthcare workers’ perceptions of resilience in hospitals.

**Employee empowerment**

Empowerment refers to “an intrinsic task motivation that reflects an individual’s orientation towards his or her work role” (Gómez & Rosen, 2001). Empowerment is used in this research to reflect one’s perception of their level of empowerment after the extreme event. One of the ways motivation is manifested is by demonstrating competence. Competence may be manifested through decision making, team work, taking responsibility, and others (Gómez & Rosen, 2001). An empowered employee makes independent decisions, solves problems, and ‘takes control’ to ensure that the organization’s objectives are achieved. We argue that because empowered employees take the initiative to complete their tasks, they are likely to demonstrate similar qualities after an extreme event by engaging in behavior that mitigates the negative consequences of the extreme event. As such, we hypothesize the following.

Hypothesis 5: Employee empowerment will have a positive effect on healthcare workers’ perceptions of resilience in hospitals.

**Emergency training**

Emergency training relates to the perceived effectiveness of emergency preparedness and response courses offered to the hospital workers. The effect of emergency training has been widely discussed and observed in previous events. A recent example is from Superstorm Sandy, where it was determined that limited training caused performance challenges during the storm (VanDevanter et al., 2014). Also, pre-incident planning activities such as training, enhance an organization’s ability to a continue operations during a disturbance. This leads us to hypothesize the following.

Hypothesis 6. Emergency training will have a positive effect on healthcare workers’ perceptions of resilience in hospitals.

**Control variables**

The control variables we use in the hypothesized model are work experience and severity of the extreme event. Severity of the extreme event pertains to the duration of the last EMR outage experienced by the participant.
Methodology

A survey instrument was developed to test the hypothesized model. The following sections describe the measures, data sample, and data collection and analysis procedures.

**Measures**

All variables used in this study were measured using multiple items anchored on a seven point Likert scale. The unit of analysis was done at the individual level. The dependent variable, resilience in hospitals, was measured using four items which were adapted from Smith et al. (2008) and modified to fit the research context. The items related to healthcare workers’ perceptions of the hospital’s ability to bounce back from an extreme event. Information privacy was formatively operationalized using four items relating to how healthcare workers perceived the effectiveness of the hospital’s privacy policies, workflow processes, privacy culture, and privacy measures after an extreme event. Following recommendations from Jarvis, MacKenzie, and Podsakoff (2003), information security was operationalized as a two-dimensional construct relating to protection from internal and external threats, and security policies regarding information sharing and access. These items were adapted from previous studies (Kim, Sivasailam, & Rao, 2004; Lee, Strong, Kahn, & Wang, 2002). We used the repeated indicator approach to measure the reflective to formative model as recommended in Ringle, Sarstedt, and Straub (2012). Information access was measured using two adapted items relating to ease of accessing and obtaining information (Lee et al., 2002). Leadership during emergencies was measured using four new items; two of those items, namely, the leader’s ability to anticipate workflow problems and avoid crisis, and empowering individual situational decision awareness, were adapted from Kayworth and Leidner (2002). The rest of the items were self-created. Employee empowerment was measured using three items adapted from Menon (2001). These included employees’ capabilities, competence, and work efficiency after the extreme event. The last variable was emergency training, which was formatively measured by three items relating to response training, training relating to the security and privacy after the extreme event, and frequency of training. The formatively measured variables were information privacy, information security, and emergency training. The rest were measured reflectively. For the control variables, work experience, was the number of years the participant has worked as a clinical or non-clinical staff. The severity of previous extreme events experienced was measured in terms of the duration of EMR outage experienced.

**Sample and Sampling Approach**

The survey was administered to hospital staff in 15 different hospitals in the Western and Central New York region. A total of 415 completed surveys were received. After removing incomplete responses, 402 data records remained and were analyzed for this research.

**Data Analyses**

The model was estimated using the PLS-SEM method in SmartPLS 3.2 (Ringle, Wende, & Becker, 2014). First, we tested the psychometric properties of the measurement scales. The reflective measures were assessed for reliability and validity. Table 1 shows that all item loadings were greater than 0.7. The values for Cronbach’s alpha, composite reliability, and Average Variance Extracted (AVE) were above 0.7. As such, the established guidelines for reliability and validity of reflective measures were met. For formative measures, it has previously been determined that estimating their reliability is not necessary, however, high correlations of indicators leads to unstable estimates, which are difficult to interpret (Diamantopoulos, Riefler, & Roth, 2008). As such, the recommendation for verifying the reliability of formative measures is by conducting multicollinearity tests (Andreev, Heart, Maoz, & Pliskin, 2009; Diamantopoulos et al., 2008). One way to test for multicollinearity is by calculating the Variance Inflation Factor (VIF), which assesses the level of variance in the estimated coefficients (Andreev et al., 2009; Diamantopoulos et al., 2008). VIF indicates the level of inflation of the standard errors due to high multicollinearity. A high VIF value is indicative of the presence of multicollinearity. According to the established guidelines, the acceptable cut off value for VIF is 10 (Diamantopoulos et al., 2008). The reliability of the formative variables in this study was therefore evaluated by testing the assumption of multicollinearity. The VIF values in Table 2 were less than the recommended cutoff value, demonstrating excellent reliability of the formative variables (Diamantopoulos, 2006).
<table>
<thead>
<tr>
<th>Variable/items</th>
<th>Item Loading</th>
<th>Cronbach Alpha</th>
<th>Composite Reliability</th>
<th>AVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perceptions of resilience in hospitals</td>
<td></td>
<td>0.907</td>
<td>0.937</td>
<td>0.79</td>
</tr>
<tr>
<td>(Res1)</td>
<td>0.954</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Res2)</td>
<td>0.927</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Res3)</td>
<td>0.915</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Res4)</td>
<td>0.744</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Leadership during Emergencies (Lead)</td>
<td></td>
<td>0.953</td>
<td>0.966</td>
<td>0.876</td>
</tr>
<tr>
<td>Lead1</td>
<td>0.95</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lead2</td>
<td>0.943</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lead3</td>
<td>0.926</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lead4</td>
<td>0.923</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee Empowerment (Emp)</td>
<td></td>
<td>0.907</td>
<td>0.942</td>
<td>0.844</td>
</tr>
<tr>
<td>Emp1</td>
<td>0.921</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emp2</td>
<td>0.921</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emp3</td>
<td>0.914</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Access (Access)</td>
<td></td>
<td>0.982</td>
<td>0.991</td>
<td>0.983</td>
</tr>
<tr>
<td>Access1</td>
<td>0.922</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access2</td>
<td>0.919</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information protection (first order)</td>
<td></td>
<td>0.819</td>
<td>0.917</td>
<td>0.847</td>
</tr>
<tr>
<td>Protect1</td>
<td>0.922</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protect2</td>
<td>0.919</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Policies (first order)</td>
<td></td>
<td></td>
<td>0.777</td>
<td>0.901</td>
</tr>
<tr>
<td>Policy1</td>
<td>0.92</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy2</td>
<td>0.89</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Validity and reliability results of the reflective variables.
Perceptions of Resilience after an Extreme Event

Table 2 Multi-collinearity assessments

<table>
<thead>
<tr>
<th>Variable</th>
<th>VIF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leadership during emergencies</td>
<td>1.82</td>
</tr>
<tr>
<td>Employee Empowerment</td>
<td>1.643</td>
</tr>
<tr>
<td>Information Access</td>
<td>1.267</td>
</tr>
<tr>
<td>Information Security</td>
<td>2.11</td>
</tr>
<tr>
<td>Information Privacy</td>
<td>2.037</td>
</tr>
<tr>
<td>Training</td>
<td>1.554</td>
</tr>
</tbody>
</table>

Results

The results of hypothesized model are shown in Figure 1. Overall, all the variables were statistically significant at a p value < .05. The strongest predictors of perceptions of resilience in hospitals were leadership during emergencies and information privacy. The results show that information privacy is more important in achieving a high level of resilience compared to information security. The weakest relationship was between information access and perceptions of resilience in hospitals.

Figure 1: PLS Path Analysis of hypothesized relationships. R² = 0.543, N = 402.

* Significance at p < .05, ** Significance at p < .01, *** Significance at P < .001.
Discussion and Future Work

We found that leadership during emergencies, information privacy, and employee empowerment had the strongest positive effect on healthcare workers’ perceptions of resilience in hospitals. This study confirms earlier findings in Waugh and Streib (2006) regarding the importance of having a well-defined leadership structure to manage all aspects of the extreme event, consequently improving the organization’s level of resilience (McManus et al., 2008). The findings also confirm the role of emergency training in enhancing the organization’s resilience as previously established Crichton, Ramsay, and Kelly (2009). Likewise, we verify that even during tumultuous environments, empowered individuals engage in behaviors that promote the hospital’s level of resilience. Based on these findings, it should be noted that the presence of leadership after an extreme event does not discourage hospital staff from ‘taking charge’ and making independent decisions as needed.

A major contribution of this research in progress is the effect of information security, information privacy, and information access on organizational resilience after an extreme event. We found that while information privacy, information security, and information access positively influence healthcare workers’ perceptions of resilience in hospitals, the strongest relationship was information privacy. Healthcare workers consider information privacy to be more critical to the effective continuity of healthcare services after an extreme event compared to both information access and information privacy. These findings have practical implications for planning and preparing for extreme events in hospitals and other service organizations. The research contributes to the organizational theory of resilience and to the literature in extreme events and business continuity.

Acknowledgements

This research has been funded by the National Science Foundation (NSF) under Grant 1241709. The usual disclaimer applies.

References


