Factors Influencing the Development of Information Systems Disaster Recovery Plan in the Ghanaian Banking Industry

Frederick Pobee, Faculty of Business and Economics, University of Pécs, Pécs, Hungary
Daniel Opoku, School of Business, Department of Human Resource, University of Education, Winneba, Ghana

ABSTRACT

Information systems (IS) have become an integral part of many organizations as they depend on it to execute their critical business function. The purpose of this research was to explore the enablers and inhibitors of information systems disaster recovery planning in organizations in the Ghanaian banking sector. In order to achieve this purpose, the protection motivation theory and the theory of planned behavior was used as the theoretical lens for this study. Eight hypotheses were developed to test the research conceptualization. Data analysis was performed using SPSS version 20.0. Using a survey of 207 managers in the Ghanaian banking sector, this article shows the factors such as perceived vulnerability, perceived severity, response efficacy, self-efficacy, attitude, subjective norms and perceived behavioral control positively influences motivation and intention to develop an information systems disaster recovery plan in Ghanaian banking industries.

KEYWORDS

Coping Appraisal, Ghanaian Banking Sector, Perceived Severity, Perceived Vulnerability, Protection Motivation Theory, Subjective Norms, Theory of Planned Behavior, Threat Appraisal

1. INTRODUCTION

Improving the efficiency and efficacy of an organization is a major reason why many organizations employ or implement information systems (Curtis, 2008; Chang, 2015). An organization’s information system is made up of the Information Technology (IT), infrastructure; people; processes and business policy and structures (Sieglar & Gaughan, 2008). A disaster recovery plan is a system of internal control and security that focuses on quick restoration of services for critical organizational processes when these operations fail due to natural or man-made disasters (Tamura, Yamamoto, Tomiyama & Hatono, 2000; Sahebjamnia et al., 2014). Disaster recovery planning is all about being prepared for potential disasters, so that when a disaster strikes, the organization’s critical functions can be maintained or resumed. The implementation of disaster recovery plans (DRPs) allows organizations to resume their business operations as quickly as possible following a disaster such as flood or fire (Levitt, 1997; Fiksel et al., 2015). Ivancevich, Hermanson and Smith (2001) argue that because most organizational activities depend on information systems, many organizations simply cannot conduct business if their information systems are not functioning. This argument concurs with Chang (2015) who further argues that if information systems are lost through disaster, this may have negative impact on the organization affected such as financial loss and loss of time to reproduce or regain

DOI: 10.4018/IJSDS.2018070107
the information system. Simply stated, the potential loss of information systems is a significant organizational risk that must be addressed by all organizations.

Information systems disaster includes deleting a file or program accidentally to a flood or fire, which destroys the building housing the data Centre (Saccomanno & Mangialardi, 2008; Rodger et al., 2015). An Information systems disaster occurs when the damage results in the information system not being to provide services (Gold, 2008; Levitt, 1997). It is also important to note that information disaster recovery plan is for returning or repairing information systems services but not essentially restoring specific hardware and software architecture (Guster, McCann, Krzenski, 2008; Schwalbe, 2010; Mete & Zabinsky, 2010). The rationale behind disaster recovery planning is to minimize potential loss by identifying, prioritizing and safeguarding the most valuable organisational assets that need the most protection (Levitt, 1997; Sembiring & Siregar, 2013). It can therefore be said that system disaster recovery planning in an organization is therefore a system for internal control and security that focuses on quick restoration of information systems for critical organizational processes when these systems fail due to natural or man-made disaster. Building a strong disaster recovery planning is the goal of every organization as it provides a host of benefits for a firm, including the resumption of critical business operations, minimization of potential loss (Kaur, 2007; Smith et al., 2018).

Limited researches though very relevant exist on the enablers and inhibitors of ISDRP in organizations (Choi & Johanson, 2012; Gopal & Gosain, 2010; Yang et al., 2017). Most of these researches focused on telecommunication industries and manufacturing industries (Mithas & Jones, 2007; Aral & Weill, 2007; Azadegan & Jayaram, 2017). While a somewhat blind eye seems to have been turned on the enablers and inhibitors of ISDRP in the banking industry. This study seeks to address this gap by exploring the enablers and inhibitors of ISDRP in the Ghanaian banking sector.

Furthermore, literature reviewed for this study revealed that research and studies on information system disaster recovery planning among organizations in the African context is limited. For instance, articles reviewed for this study revealed that only three studies arguably were focusing on ISDRP among organization in the African context (Kgakats & Rautenbach, 2013; Raju & Niekerk, 2013). However, these studies focused on ISDRP among the telecommunication industries in South Africa. Whereas studies on ISDRP are far advanced in other continents, Africa needs more research on ISDRP in order to contribute to literature and knowledge (Klein & Rai 2009; Schubert & Legner, 2011; Pollock & Williams, 2009; Coetzee et al., 2018; Lumbroso, 2018). In order to fill this context gap, this study will explore information systems disaster recovery planning among organization in the Ghanaian banking sector.

2. RESEARCH FRAMEWORK

The research adopts of the tenets of the Protection Motivation Theory (PMT) and the theory of planned behavior (TPB) to study ISDRP. The two theories; the theory of planned behavior (Ajzen, 1991) and the protection motivation theory (Rogers, 1983) was integrated to increase our knowledge of ISDRP by employees and managers in modern organizations.

2.1. Protection Motivation Theory

The Protection Motivation Theory (PMT) states that the motivation of the stakeholders to protect themselves from harm is enhanced by the following five perceptions:

A. The severity of the threat,
B. Their vulnerability to the threat,
C. Self-efficacy, i.e., their confidence in their ability to cope with the threat and perform threat reducing behaviors,
16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage:

www.igi-global.com/article/factors-influencing-the-development-of-information-systems-disaster-recovery-plan-in-the-ghanaian-banking-industry/208683?camid=4v1


Recommend this product to your librarian:

www.igi-global.com/e-resources/library-recommendation/?id=159

Related Content

Intellectual Property Regulation, and Software Piracy, a Predictive Model
Michael D'Rosario (2016). International Journal of Strategic Decision Sciences (pp. 21-34).
www.igi-global.com/article/intellectual-property-regulation-and-software-piracy-a-predictive-model/170605?camid=4v1a

Performance Measurement: From DEA to MOLP
www.igi-global.com/chapter/performance-measurement-dea-molp/11312?camid=4v1a
Business Models in Modern Competitive Scenarios: The Role of Information in the Formulation of the Strategy
[www.igi-global.com/article/business-models-in-modern-competitive-scenarios/208678?camid=4v1a](www.igi-global.com/article/business-models-in-modern-competitive-scenarios/208678?camid=4v1a)

Forecasting Direction of the S&P500 Movement Using Wavelet Transform and Support Vector Machines
[www.igi-global.com/article/forecasting-direction-p500-movement-using/77337?camid=4v1a](www.igi-global.com/article/forecasting-direction-p500-movement-using/77337?camid=4v1a)