UNIVERSITY OF GHANA

ENABLERS AND INHIBITORS OF INFORMATION SYSTEMS DISASTER RECOVERY PLANNING: EVIDENCE FROM MANAGERS IN THE GHANAIAN BANKING SECTOR.

BY

FRED POBEE
(10245437)

THIS THESIS IS SUBMITTED TO THE UNIVERSITY OF GHANA, LEGON IN PARTIAL FUFILMENT OF THE REQUIREMENT FOR THE AWARD OF MPHIL MANAGEMENT INFORMATION SYSTEMS DEGREE

JULY, 2014

DECLARATION

I do hereby declare that this work is the results of my own research and has not been presented by anyone for any academic award in this or any university. All references used in the work have been fully acknowledged.

I bear sole responsibility for any shortcomings.

FRED POBEE **23/07/2014**

(10245437) **DATE**

CERTIFICATION

I hereby certify that this thesis was supervised in accordance with procedures laid down by the University.

…….. ……

DR. ERASMUS ADDAE DATE
(SUPERVISOR)

…… ……

DR. RICHARD BOATENG DATE
(CO-SUPERVISOR)

DEDICATION

This study is first and foremost dedicated to the Almighty God who has given me the strength, good health, wisdom as well as life for me to see this day. Secondly, it is also dedicated to my dad, Mr. Francis E.S. Pobee and my mum, Mrs. Augustina Pobee, and all my course mates who have been very helpful throughout the duration of this course.

ACKNOWLEDGEMENTS

It can be said that no one completes a thesis alone, and for me this could not be a more true statement. First, I owe special gratitude to Dr. Erasmus Addae, my supervisor. His guidance, mentorship, and belief in this project were critical to its completion. There is no doubt about his unparalleled and unmatched dedication to service. Additionally, very special thanks go to Dr. Richard Boateng who in addition to my supervisor, co-supervised me and provided guidance for this research. Thank you all for your assistance, teaching, and reading as well as for the many comments you provided over the past few months. Without you, this project may have never got off the ground. Additionally, I would like to acknowledge the support of my head of department (H.O.D), Dr. John Effah towards the completion of this research project.

A big thank you to all the firms and respondents who made time out of their busy schedule to respond to my questionnaire. Especially to Mr. Essel of Standard Chartered bank am very grateful for your assistance. To Mr. Ofori-Teiko also of Cal bank, I say God richly bless you for your advice and assistance.

To my family who have always believed in me, especially my mum and dad, who through their discipline instilled in me the virtues of hard work and honesty, your unwavering love for me is a cornerstone for the man you see today. Thank you for always encouraging my curiosity.

To friends and mentors near and far, thank you for reading the many drafts and providing such wonderful encouragement and feedback. Most of all, thank you for your support.

To my Heavenly Father, my God, I am so very blessed. My cup runs over with your Grace, Mercy, and Love. To you be the glory and through you, all things are possible.

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

BCP	Business Continuity Planning
DRP	Disaster Recovery Planning
IS	Information Systems
ISDR	Information Systems Disaster Recovery
ISDRP	Information systems Disaster Recovery Planning
PMT	Protection Motivation Theory
TPB	Theory of Planned Behavior
IT	Information Technology

LIST OF TABLES

TABLE **PAGE**

LIST OF FIGURES

FIGURE **PAGE**

ABSTRACT

Information systems (IS) have become an integral part of many organisations as they depend on it to execute their critical business function. As a result any situation that will render the IS unavailable will be detrimental to most organisations. The purpose of this research was to explore the enablers and inhibitors of information systems disaster recovery planning (ISDRP) in organisations in the Ghanaian banking sector. In order to achieve this purpose, the study used the quantitative method to investigate the enablers and inhibitors of Information Systems Disaster Recovery Planning. Seven banking organisations were used in the survey. Integrating the protection motivation theory and the theory of planned behavior, several hypotheses were developed to test the research conceptualization. Data analysis was performed using SPSS. Using a survey of 207 managers in the Ghanaian banking sector, this study showed the factors such as perceived vulnerability, perceived severity, response efficacy, self-efficacy, attitude, subjective norms and perceive behavioral control positively influences motivation and intention to develop an ISDRP in Ghanaian banking industries. Eight hypotheses were formulated to investigate the enablers and inhibitors of ISDRP. The data analysis did not support response cost as being a predictor of motivation and intention to develop an ISDRP in the Ghanaian banking industries.

This study adds up to the few existing studies in the field of IS that have studied a phenomenon by integrating the two aforementioned theories. This study discussed information systems disaster recovery planning (ISDRP) among organisation in the Ghanaian banking sector. However, future research can extend this work by looking ISDRP from other financial institutions, for example among insurance companies and so on.

Keywords: Information systems, disaster recovery planning, protection motivation theory, theory of planned behavior.

CHAPTER ONE

INTRODUCTION

1.1 Research Background

Improving the efficiency and efficacy of an organisation is a major reason why many organisations employ or implement information systems (Curtis, 2008). An organisation'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 organisational processes when these operations fail due to natural or man- made disasters (Tamura, Yamamoto, Tomiyama and Hatono, 2000). Disaster recovery planning is all about being prepared for potential disasters, so that when a disaster strikes, the organisations' critical functions can be maintained or resumed. The implementation of disaster recovery plans (DRPs) allows organisations to resume their business operations as quickly as possible following a disaster such as flood or fire (Livitt, 1997). Ivancevich, Hermanson and Smith (2001) argues that due to the fact that most organisational activities depend on information systems, many organisations simply cannot conduct business if their information systems are not functioning. Simply stated, the potential loss of information systems is a significant organisational risk that must be addressed by all organisations.

Information systems disaster includes deleting a file or program accidentally to a flood or fire which destroys the building housing the data Centre (Saccomanno and Mangialardi, 2008). 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 (Gustav, 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 (Livitt, 1997). From the above, we can say that an information system disaster recovery planning in an organisation is therefore a system for internal control and security that focuses on quick restoration of information systems for critical organisational processes when these systems fail due to natural or man-made disaster. Building a strong disaster recovery planning is the goal of every organisation as it provides a host of benefits for a firm, including the resumption of critical business operations, minimization of potential loss, and so on (Kaur, 2007).

Information systems disaster has an effect on the organisation that employs the information system (Schubert and Legner, 2011); including those information systems services which is outsourced to independent vendors (Curtis, 2008). Harney (2004, p. 42) argued that "if the vendor somehow fails to provide an effective information systems service, its client may be faced with information systems disaster". Organisations that have a disaster recovery plan in place recover 2.5 times faster after a disaster than companies without one (Fabian & Dhillon, 2007). This shows how essential disaster recovery plans are for an organisation. Helping an organisation recover after a disaster means continuing with business activities and not losing money. However, a study by CEO's in the U.S. found that 50% of them had a plan in place to manage disaster, though 89% believed that "a crisis is as certain as death and taxes", (Schubert and Legner, 2011). Disaster is therefore regarded by managers as an inherent component of the organisation which is bound to happen but what will make the difference is

the ability of the manager to put measures and plans in place to tackle the disaster, put the organisation in its right shape and continue with business operations (Aziagba and Edet, 2008).

Most often than not information systems disaster recovery planning (ISDRP) is not given the necessary attention in business organisations. Grigonis (2002) argues that even though sophisticated information systems are evident in modern organisations, their information systems disaster recovery plan may be limited.

1.2 Research Problem

One of the problems that have plagued systems managers in recent times is the effect on the business and its information systems if a disaster were to strike the organisation (Robb, 2005). In particular information systems managers are expected to make arrangements and put measures in place for backup facilities to resolve a damaged system. Housel, Sawy & Donovan (2006) argue that disaster recovery plan (DRP) is important or relevant because no organisation is immune to disaster or crisis. Every organisation is prone to disaster. Organisations must therefore set up DRP to put the organisation on its feet if it gets stricken by a disaster.

Managers including information systems managers are becoming increasingly concerned with the effect on its information systems and business if a disaster were to strike the organisation (Day, Junglas & Silva, 2009). While information systems disaster recovery planning is occasionally addressed in information systems textbooks (Hiltz, Van de Walle, & Turoff, 2010) and is generally regarded as an important managerial activity (Kovacs and Spens, 2010; Ramsaran, 2005), it is rarely approached in mainstream research. For instance, a

study by Shrosphire and Kadlec (2009), on developing the IT disaster recovery planning construct highlights a three part study in which the creation of a domain definition precedes the development and evaluation of an empirically reliable and valid measure of IT disaster recovery planning. They followed a previously validated framework to create a 7 dimension, 34 item measure for assessing the degree of IT disaster recovery planning. The 7 dimensions were (IT disaster identification and notification, preparing organisational members; IT services analysis, recovery process, backup procedures, offsite storage, and maintenance). The measure was validated using a sample of 153 banking and finance firms. The result of the study led to a conceptual definition of IT disaster recovery planning which an organisation follows in order to improve its ability to resume IT services following a disaster. However, Shrosphire and Kadlec (2009), focused solely on revamping IT infrastructure (which is just a component of an IS). This research extends their study by looking at ISDRP as a whole of which IT is part of.

Limited researches though very relevant exist on the enablers and inhibitors of ISDRP in organisations (Choi and Johanson, 2012; Gopal and Gosain, 2010). Most of these researches focused on telecommunication industries, manufacturing industries and so on (Mithas and Jones, 2007; Aral and Weill, 2007). 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 organisations in the African context is limited. For instance in reviewing articles for this study it was found that only three studies arguably were focusing on ISDRP among organisation 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 bridge the gap with the other continents like Europe and Asia (Klein & Rai 2009; Schubert & Legner, 2011; Pollock & Williams, 2009). In order to fill this context gap, this study will explore information systems disaster recovery planning among organisation in the Ghanaian banking sector.

1.3 Research Purpose

The purpose of this research is to explore the enablers and inhibitors of information systems disaster recovery planning in organisations in the Ghanaian banking sector.

1.4 Research Objectives

The objectives of the study are:

1. To investigate the awareness of ISDRP among organisations in the Ghanaian banking sector.
2. To investigate the enablers and inhibitors of information systems disaster recovery planning among organisations in the Ghanaian banking sector.

1.5 Research Questions

1. What is the extent of awareness of ISDRP in organisations in the Ghanaian banking sector?
2. What are the enablers and inhibitors of information systems disaster recovery planning in organisations in the Ghanaian banking sector?

1.6 Significance of the Study

The study integrated the theory of planned behavior and the protection motivation theory to investigate the ISDRP among managers in the Ghanaian banking sector.

Findings and results reported in this study will provide a more reliable way of developing a disaster recovery plan for information systems.

Also the study will provide feedback on policies driving the development and implementation of information systems disaster recovery plan to the operations of other organisations that have interest in employing information systems.

1.7 Chapter Disposition

The organisation of the research was as follows:

Chapter one (1): Introduction

This chapter provided a basis for the research by giving an overview of the background, the problem statement, research purpose, the research objectives, the research questions, the significance, research limitation and Organisation of the research.

Chapter two (2): Literature review

Literature pertaining to information systems disaster recovery planning was reviewed. This was done to synthesize and also make comparative analysis on arguments raised concerning information systems disaster recovery planning.

Chapter three (3):

This chapter presents a brief overview of the banking sector in Ghana. It also discussed information systems disaster recovery planning in the Ghanaian banking industry.

Chapter four (4): Research framework

This chapter provided the research framework which was adopted for this study. The constructs and variables of the framework were explained followed by how they will be measured. This chapter is important as it provides the frame for the research.

Chapter five (5): Research methodology

This chapter describes the research methodology adopted which included research design, data collection procedure and development of data collection instruments. Mode of data analysis will also be outlined in this chapter.

Chapter six (6): Data Analysis and Discussion of Findings

This section explored the data collected from the field and was analysed using multivariate techniques and thematic analysis. Empirical findings based on information systems disaster recovery planning were presented in this chapter.

Chapter seven (7): Summary, Conclusions and Recommendation

The final chapter presented a summary of the principal findings, and contributions made to the study of information systems disaster recovery planning in the Ghanaian banking sector. Implications for managerial practice and recommendations for future research were also highlighted in this section.

1.8 Summary

This chapter provides the background of the research study, the study purpose, objectives, research questions, the research methodology and the research significance. The next chapter will provide a literature review of the research study.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction/Background and Rationale for the Review

Organisations have become more reliant on information systems (IS) which is becoming integrated into all parts of organisations (Philpott, 2007). This review builds upon a succession of reports from academic and scholarly articles that highlight the potential of information systems in organisations and the consequences of disaster on the IS of organisations. Belief in the potential of IS to help meet organisational needs (Boin & McConnell, 2007) has been driven by rapid growth in the structure of organisations and also in technology over the last decade. Because of the fact that IS has become an integral part of most organisations, any adverse effects on the organisations IS (Souliotis & Papadakis 2007) resulting from disaster being it natural or man-made may prevent the organisations from successfully reaching their goals or objectives.

The rationale behind this review is to synthesize available resources on IS and DRP. There has been a number of research on IS and DRP (Romano, Pick and Roztocki, 2010; Klein and Rai, 2009; Luo, 2007). Research indicates that most businesses readily acknowledge that disaster recovery, particularly for information systems, is a serious issue for the survival of an organisation (Lee and Panteli, 2010; Gao, 2011). Unfortunately, the language of disaster recovery to them is grindingly boring thus at the mere mention of disaster recovery, many people who are otherwise alert and intelligent tune out, with eyes glazed over (Kovacs and Spens, 2010). Others dislike the emphasis on negative or emergency scenarios. They prefer denial; pretending that their organisation will escape major disasters and believe that speaking about negative possibilities only engenders more negative thinking (Leidner, Pan

and Pan, 2010). Many firms take a giant step, burying their head in the sand and pretending not to see the impending disaster. What some researchers have done is to bring to the awareness of businesses and managers that IS disasters can occur at any time and that they should be ready for it. This research extends these studies by looking at and addressing the factors that would lead to an intention to develop an information system disaster recovery plan in the Ghanaian banking organisations.

This chapter seeks to assess the current literature on information systems and disaster recovery planning in organisations. Thus, the overall aims are as follows:

1. Provide a literature review and analysis of research concerning information systems disaster recovery planning in organisations.
2. Categorize and analyse conceptual approaches for understanding ISDRP.
3. Categorize and assess the methodologies used to carry out research studies, and evaluate the evidence from those studies.
4. Identify key research trends and gaps relating the issues addressed methodologies and concepts.

This review is important given there is growing global interest in the role IS plays in organisations (Busquets, 2010) and that disasters have also become an inherent component in organisations (Bharosa, Lee and Janssen, 2010). A number of studies have been conducted on the subject matter some of which are academic, but with a greater emphasis on adoption of ISDRP. Consequently, academic research and conceptual understanding of motivation for developing ISDRP is lagging. This is recognized in a discussion paper by Day, Junglas and Silva (2009) and Maitland, Tchouakeu and Tapia (2009) who identifies lack of motivation as a factor that impedes organisations from developing an ISDRP.

This chapter will build upon previous analyses and take stock of accumulated evidence and experience by seeking to provide a more structured approach to analyzing the literature and identifying trends and gaps in order to map out a research agenda for information systems disaster recovery planning.

2.2 Framing IS Disaster Recovery Planning Research

2.2.1 Disaster Recovery Planning Defined

This section presents the conventional wisdom on disaster recovery planning. While disaster preparedness focuses on the steps a company should do in the event of a crisis, disaster recovery focuses on the continuation and restoration of essential systems within the information systems infrastructure (Thomas and Kopczak, 2007). The two methodologies are interdependent and build upon each other. Where daily business operations are affected by unforeseen events, more is at stake than just losing money (Schulz and Blecken, 2010). A company's reputation, client assets, proprietary assets, and personnel are just as susceptible to loss (Kovacs and Spens, 2007). For any firm great and small, taking the right course of action can mitigate loss of company assets and save a business from going under. Selecting the right course of action is where disaster preparedness and disaster recovery planning begin.

A disaster according to Romano et al. (2010) need not be catastrophic to cause a business disruption. While earthquakes, flooding, and fires are detrimental to business, in reality, it does not take much for a disaster to happen (Thomas and Kopczak, 2007). A disaster is a serious disruption in a community or a society causing material, economic, social or environmental losses that go beyond the ability of the affected society to cope using its own resources (Bharosa et al., 2010). These disruptions (disaster) can therefore prevent organisations from reaching their full potential in the provision of goods and services. A

disaster, according to Klein and Rai (2009) causes severe hazard impact, damage, casualties and disruptions to a population. This assertion is supported by ISDR (2004), p.4 that defines a disaster as "a serious disruption of the functioning of a community or a society causing widespread human, material, economic or environmental losses which exceed the ability of the affected community or society to cope using its own resources". Thus a disaster can cause an organisation significant loss if the necessary disaster recovery plan is not put in place. The population which is hit by a disaster can be disadvantaged if the necessary disaster recovery planning strategies are not put in place. For example, the statistics of recorded disaster data (UNISDR, 2012) show that in 2012, 375 disasters were recorded while 9,655 people were killed and an amount of US$ 157 billion was lost. A disaster recovery plan (DRP) strategy is a system for internal control and security that focuses on quick restoration of service for critical organisational processes when there are operational failures due to natural or man-made disasters (Hiltz, Van de Walle and Turoff, 2010). A DRP aims to minimize potential loss by identifying, prioritizing and safeguarding those organisational assets that are most valuable and that need the most protection. Disasters create a dangerous situation that threatens or has the potential to cause injury to life, damage to property or the environment (Nawaz and Zualkeman, 2009).

2.2.2 Information System Disaster Recovery Planning (ISDRP)

ISDRP is the process an organisation uses to recover access to its software, data, network and hardware that are needed to resume the performance of normal, critical business after the event of either a natural disaster or a disaster caused by humans (Cumbie, 2007). Disaster primarily affects availability, which affects the ability of the staff to access data and access working systems, but a disaster can affect the other two tenets: confidentiality and integrity (Muller and Chua, 2012). Bonner, Teng and Nerur (2010) added that the confidentiality,

integrity and availability of information system must be ensured to protect the business from the risk relating to information technology. Since IS comprises of IT infrastructure, people, processes and business policy and structure, any occurrences that may distort these components of proper functioning may be referred to as an information system disaster.

Although the phrase information systems disaster recovery planning and business continuity planning are occasionally used interchangeably, they are separate processes (Anderson, 2008; Crove, 2008). For instance, plans for keeping businesses operational following a disaster is referred to as business continuity plan (BCP) (Drechsler and Natter, 2012). A business continuity plan is a road map for continuing (Ketterer and Price, 2007) operations under adverse conditions such as storm, crime, theft and so on. It identifies an organisations exposure to internal and external threats and brings together soft and hard assets to provide effective prevention and recovery for the organisation, while monitoring competitive advantage (Kovacs and Spens, 2010). On the other hand information systems disaster plan are aimed specifically at revamping information system services after a disaster (Wakolbinger and Toyasaki, 2011). It can therefore be deduced that information systems disaster recovery plan (ISDRP) supports business continuity plan (BCP) and that ISDRP is a subset of BCP. And the rationale behind ISDRP and BCP should not be conflicted.

2.2.3 Overview of IS DRP Process

The issue of ISDRP has received some amount of attention in literature (Kaplan and Haenlein 2010; Lai and Turban 2008; Hoffman and Novak, 2012). This session of the review is intended to give a critical and comparative analysis of the fundamental and important elements of developing and implementing an ISDRP. Below is the discussion on the process for ISDRP.

1. *Define Key Assets, Threats and Scenarios.* According to Crowe (2010) ISDRP effort should start with identification of key assets, and definition of the business impact of loss of each asset. This assertion concurs with Boyd and Ellison (2008) argument that definition of key assets, threats and scenarios is a critical step in that you need to know what IS assets you're protecting and what its value to the business is, to define how it should be protected. Miller (2010) supports the above arguments by indicating that this exercise allows you to determine, based on the impact of loss, the appropriate protection required for each IS asset. Geographical location of organisations can bring its attention to the kind of disaster threats that exist (Reuter, Heger and Pipek, 2012). An organisation in New York City, for example, does not need to be very concerned about the threat of earthquakes, but does have more concern around terrorism than an organisation headquartered in Japan. Potential threats to be considered and mitigated against are outlined in Table 2.1

Table 2.1

The two major types of disaster

Natural Threats	Man-made Threats
a. Fire	a. Terrorism
b. Flood	b. Explosion
c. Hurricane/Storm	c. Theft/Vandalism
d. Earthquake	d. Riot
	e. Hardware Failures
	f. Software Failure
	g. User errors
	h. Process Failure
	i. Policy Errors

Source : (Reuter, Heger and Pipek, 2012).

2. *Determine The Recovery Window*. Once an organisation has defined its IS assets, it needs to determine how long it can go without access to these assets. This is called the "Recovery Window" for each asset (Crowe, 2010). Clearly the recovery plan is going to be very different (and less expensive) if the IS assets can be unavailable for 3-5 days following disaster, versus a mandate of being up within 3-5 hours (Idugboe, 2011). Some of the organisations information systems may have a 1 hour (or less threshold), while others may be fine if they are operational the next day, and this allows the IT team (Rice, 2012) to focus on the most important systems first. This requires consensus and input from top management.

3. *Define Recovery Solutions.* The third step builds upon the first two, and here the organisation must define the appropriate approach and solutions for recovery based on the assets and the recovery window (Sutton, 2009; Ahmed, 2011). Solutions can include recovering from tape backup or disk backup, or data replication to an offsite location (Schwalbe, 2010). For example, an e-commerce web site may need to be operational at all times since it is customer-facing, and this dictates co-location and possibly data replication (Pokharel, 2011). Each IS asset, based on its defined value and recovery window, can then have an appropriate disaster recovery solution identified, with a commensurate budget that maps back to business value and impact (Leydesdorff, 2010).

4. *Draft A Disaster Recovery Plan.* Drafting of the ISDRP will be defined by the assets and how they will be protected, but will also address key process and communication-related elements (Pokharel, 2011). Furthermore, the process for assessing damage to

the existing site, as well as mitigating/minimizing damage, needs to be considered (Van, Turoff and Hiltz, 2010). An important element of the disaster recovery plan according to Van et al. (2010) is establishing an emergency operations centre – a location where employees and stakeholders responsible for executing on the DRP can converge to in order to work together and have access to resources and decision-making authority. This location should be pre-established and have resources including office supplies, telecommunications, food and water, communications lines and other needed tools (White, 2011). FEMA (2009) indicates that the most important rule of disaster recovery planning is "People First." In other words, the safety of an organisational employees and personnel is always a more important consideration than saving assets or business recovery operations. It is important that ISDRP team understand this, and that they make it a consistent element of their planning and message.

5. *Establish A Communications Plan and Assign Roles.* The fifth step in the ISDRP process is identifying the communication plan and assigning roles and responsibilities to member of your disaster recovery team (Sutton, 2009). From a communications standpoint it is important to have a well-organized, accurate and up-to-date list of contacts for each function or role. Including emergency contact home and cell phone numbers, email addresses and a chain of communications so instructions can be distributed hierarchically. It is important to be able to move quickly, and efficient communication is the key to this (Aggelinos & Katsikas 2007). Employee training is absolutely critical. Once people know what their roles are, it is important that they know how to execute on their tasks, who to escalate issues to or seek instruction from, and where to find the most current version of the plan (Shaluf, 2007). On the contrary,

if people are not trained, and clear on their responsibilities, the actual disaster scenario will go very badly (Ahmed and Sugianto, 2008). Many organisations do not have the resources in-house to deal with all of the different roles and elements of executing the disaster recovery plan (Eshghi and Larson, 2008), which means that outside organisations may play key roles in executing on the DRP. When that is the case, it is critical that these vendors understand their role in the plan, and that service level agreements are in place so those organisations are properly prepared and resourced to assist you with execution (Marincioni, 2008).

6. *Document The Disaster Recovery Plan, In Detail.* The six step is an absolutely critical one were the organisation must document the DRP. Although the organisation must have developed a draft disaster recovery plan in step 4 above (Ahmed and Sugianto, 2008), in this step it is important to develop a more detailed plan for each system on exactly what to do to implement failover to the IS Disaster Recovery site system. Barbara (2008) highlighted that an IS disaster recovery plan needs to be very specific and detailed because in the middle of an organisational crisis, room is not left for open interpretation (Sagun, Bouchlaghem and Anumba, 2008).

7. *Test The Disaster Recovery Plan.* Only through a real test will the staff and management be familiar with what to do in the event of a disaster, but equally important, through this process organisations can identify the gaps, inconsistencies and errors in the plan (Miller, 2010). It is much better to identify problem areas in a test than in a real disaster. Again, you don't want to leave things open to interpretation in the middle of a pressurized, stressful situation.

8. *Refine and Re-Test the Disaster Recovery Plan*. Finally, the 8th Step is to refine the plan and its documentation, and conduct a re-test based on this revised and refined version. The re-test should be much smoother than the first, and should put you in a position where you are ready to execute against the plan in a real disaster recovery situation.

2.2.4 Classification of ISDRP Research

In this chapter, we define ISDRP as the process an organisation uses to recover access to its software, data, network and hardware that are needed to resume the performance of normal, critical business after the event of either a natural disaster or a disaster caused by humans (Cumbie, 2007). Moving on from this definition, the study can give a brief overview of research classification in the literature on ISDRP:

a) Issues that have been discussed in relation to ISDRP include adoption of ISDRP, development of ISDRP, implementation of ISDRP and evaluation of ISDRP. Much of the literature especially the earlier literature in the period under review is characterized by write ups on the adoption and motivation for ISDRP in organisations. Subsequently, a number of works have focused on advantages and benefits organisations stand to enjoy when they adopt ISDRP (Fajardo and Oppus, 2010). Hence, this study argues that works on ISDRP adoption represent one of the enduring themes of ISDRP research.

b) The methodological approaches identified in the ISDRP literature include qualitative, quantitative and mixed method approaches. Evidence of this from the ISDRP literature shows that all three methodological approaches have been used extensively in ISDRP research.

c) Furthermore, classification was also done based on the geographical regions. Regions like Asia and Europe dominated with research works on ISDRP whereas Africa was the least among the regions with researches on ISDRP.

d) Additionally, theories or frameworks used in the ISDRP researches within the years specified were also classified. Models like the contingency model, emergency management model, protection motivation theory and the theory of planned behavior were frequently used in various studies.

On the basis of the above discussion and with reference to previous works, the classification framework shown in Figure 2.1 is developed to guide the analysis in this chapter. In investigating each of the themes in Figure 1 and the issues identified under them, previous works on these themes were analyzed. For each of the issues, the study would identify and discuss the research that has been done on the issue. First, we would briefly explain each one of the research themes and related issues identified.

Figure 2.1 Classification framework

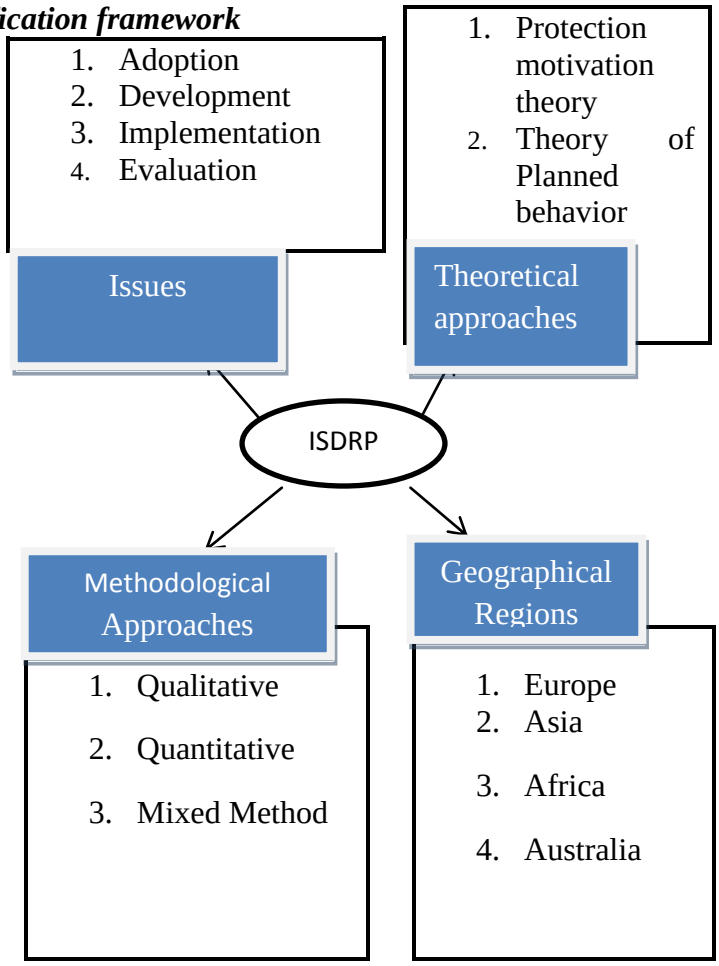


Figure 2.1 shows the themes discussed under ISDRP and the issues discussed under them. Figure2.1 will guide the analysis in this chapter. Methodology for the literature review can be found in Appendix C.

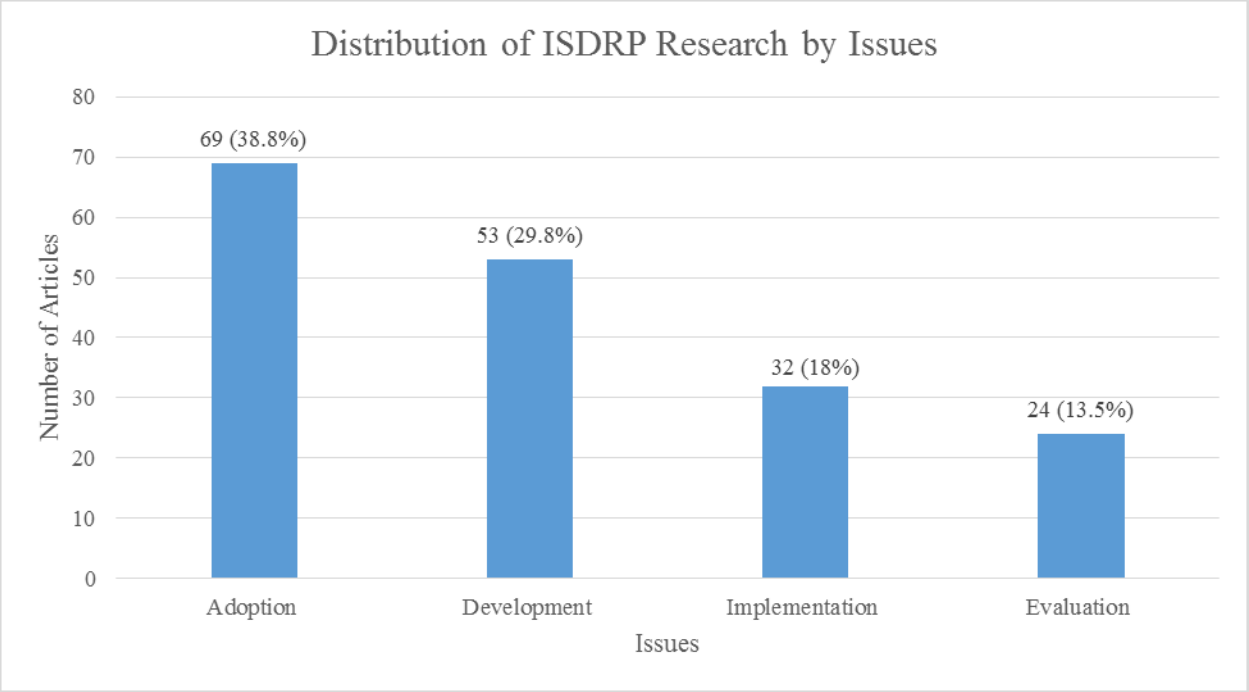
2.3 Mapping ISDRP Research: Issues and Evidence

A total of 178 articles from a spectrum of IS journals were classified according to the classification scheme developed from the literature review. The researcher begins the mapping of the previous research on ISDRP by identifying the issues that have be discussed and researched. Drawing from the literature, four issues; motivation, development,

implementation and evaluation of ISDRP were identified and used as the initial classification schema.

Distribution of ISDRP research by issues

Figure 2.2



As illustrated in the figure above, the findings classify previous research ISDRP in four sub-categories. There is a dominance of research in the adoption and motivation for ISDRP (38.8%) and ISDRP development (29.8%) and this is followed by implementation of ISDRP (18%) and ISDRP evaluation (13.5%). The dominance of literature on the adoption and motivation for ISDRP demonstrates the phases the ISDRP has gone through or is going through with that issue in question. Most studies illustrates that organisations are becoming increasingly aware of the consequence of disaster on their operations and information systems (Kovacs and Spens, 2010; Simchi-Levi, 2008) as a result many of these organisations have adopted various ISDRP.

Table 2.2 Mapping of articles surveyed according to issue and factors the drive and inhibits ISDRP

Factors	Adoption	Development	Implementation	Evaluation
Group 1-Enablers of ISDRP				
Active support of senior management	11, 26	14	15	18, 8
Commitment of funding	20	25, 2	22, **16**	**12**
Protection of information assets	7	8, 13	10, 15, 8	5
Negative experience(s) can drive change	14, 11	**12**	**41**, 37, 43	27, 18, **16**
Staff awareness and training	22, 7	43, 5	14	**19**, 27
Standards and legislation for vital records may be enforceable	22, 11	25	14	8, 37
DRP processes to encompass the whole organisation (so every employee must be involved)	43	**12**	**23**, 27	**19**
Group 2- Inhibitors of ISDRP				
Lack of management awareness	**12**,8	**23**	25,37	13
Lack of security awareness and training for all staff	17	24	**41**, 43	**23**
Lack of allocated funds due to low priority	8	13, 27	**19**	**16**, 11
No negative experiences so it is assumed that everything is okay	33, **41**	33	14,**19**	24
Lack of capacity / resources to test DRP	8	**42**, 8	45	18
Lack of current and appropriate DRP processes	15	37	45, 5	13
Expectation of users to be able to access all information when they want.	13	**41**, 27	22	**19**, 11

Bold: studies analyzing primary data

See Appendix C for reference to article number

2.3.1 Adoption/Motivation of ISDRP

This session refers to literature and research which discusses the adoption is ISDRP. The increasing adoption of IS by organisations in all industries has led them to install IS which, most of the times, are "suited" to their needs (Klein and Rai 2009). Schubert and Legner, (2011) concurred with this assertion when they indicated that majority of firms activities revolve around IS and that having a properly installed IS in an organisation reduces the cost of operations if the IS is aligned with organisation's strategy. Since IS has now become part of organisations, they cannot operate without being supported by the IS (Howden, 2009). Mete and Zabinsky (2010) states that because organisations will find it extremely difficult to operate or carry out its functions without a properly installed IS, he opined that organisations will in that same like find it difficult to carry out its activities if its information system is struck by a disaster. To help solve this organisational predicament Boin, Kelle & Whybark, (2010) in examining information sharing under co-opetition in disasters showed that firms and organisations must adopt measures to inculcate DRP when installing information systems. This will result in the organisation being able to retrieve its critical business functions should disaster strike.

Furthermore, managing interorganisational and international collaboration has garnered substantial scholarly attention (Kachra and White, 2008; Fabian and Dhillon, 2007; Little, 2010). At the forefront of aforementioned research is the recognized role that IS-enabled information sharing plays in the success of coordination and cooperation (Paul and Nazareth, 2010) especially in the advent of a disaster. However, the vast majority of research on interorganisational information sharing during IS disaster is based on the premise of a relatively stable and consistent economic and political environment, supported further by the development of long-term trusting relationships (Boin et al., 2010).

Organisations have become more reliant on information technology/information systems which are becoming integrated into all parts of those organisations (Kovacs and Spens, 2010). This puts greater emphasis on the IT professional and the IS analyst to keep the services provided by the technology and systems working at all times. In the U.S., regulations such as Sarbanes-Oxley and HIPAA require some organisations have a disaster recovery plan. Most organisations according to Fajardo and Oppus (2010) have also taken it upon themselves to adopt a DRP for their IS so that they are not left out of operation when disaster strikes their organisation. What these studies did was to highlight and discuss the factors that lead an organisation to adopt an ISDRP.

ISDRP face technological, managerial and organisational challenges which constrain the adoption of ISDRP (Fajardo and Oppus, 2010; Little, 2010). For example Fajardo and Oppus (2010) in assessing ISDRP challenges noted the underdeveloped state of some information systems makes it difficult to align disaster recovery planning with IS. Even if this happens the technological challenges associated with it possess a challenge to the DR process (Little, 2010).

Brynjolfsson and Schrage (2009) identify lack managerial awareness on ISDRP as an inhibitor on the adoption of ISDRP. As indicated by Gordon and Tarafdar (2010) it is senior management that is ultimately accountable and charged with the task of initiating and supporting important projects with adequate funding and resources. So if managers are not made aware of ISDRP it is likely the plan would not materialize but even if it does it will not receive the necessary support it deserves.

A key enabler of ISDRP according to Aral and Weill (2007) is commitment of funding. Funding is a major factor that determines how far an organisation can realize or achieve its projects. Mithas and Jones (2007) posited that sufficient funding motivates workers and employees to give all their best knowing very well that their effort will result in a profitable outcome. If enough funds is allocated to ISDRP, there is a high tendency that the planning process will be effective and not be shawn along the way (Kohli, 2007).

2.3.2 Development of ISDRP

This session refers to literature and research which discusses the development of ISDRP. According to Pollock & Williams (2009), the process of developing an information system disaster recovery plan involves a strategic planning since DRP encompasses all aspects of the organisation. This assertion was supported by Sawyer & Winter (2011) when he argued that for a very successful ISDRP, management should have a better stake in it, this shows the importance of management in the planning and development of an ISDRP. Tilson, Lyytinen, and Sorenson (2010) further researched the difference between organisations that strategically plan for ISDRP and organisations that develop DRP without much emphasis on management. His findings revealed that half of those organisations without a strategic plan for IS disaster struggle to get back to their former state as compared to those who have. This clearly indicates that the role of management in the development of an information systems disaster recovery planning cannot be over emphasized.

The average business in China, according to Yoo (2010), has its entire system shut down nine times per year. This statement concurs with Tiwana (2012) opinion that 50% of those firms whose critical business systems go down for 10 days or more never recover and 93% of the companies with no recovery plan fail within five years. Furthermore, the costs associated with system outages due to disaster are considerable: IS downtime costs the USA $4 billion

annually, and the average cost per four hour outage is US $30,000 (Khan, 2011). Despite its importance, empirical research on the development of IS disaster recovery planning is sparse. Prior research has focused on the adoption of ISDRP by organisations (Slaughter & Kirsch, 2013). However, there is a need for a more rigorous research on the development of ISDRP in organisations.

ISDRP also faces challenges which constrain its development (Hopkins, 2010; Han and Mithas, 2011). For example, Hopkins (2010) opined that lack of security awareness and training for all staff could be an inhibitor to a successful development of ISDRP. Training of staff on ISDRP is a very critical issue in organisations since the plan against disaster has to be designed and implemented by the staff of the organisation. Han and Mithas, (2011) presented that inadequate training of staff also leads to loop holes in the disaster recovery plan. Further, lack of security awareness can also hinder the development of ISDRP in that the employees or managers will not see the reason why they should provide security for their information assets. All these without any doubt can be said to hinder a successful development of IS disaster recovery planning. And this can affect the operations of organisations. Furthermore, because organisations might not have experienced any disaster, they might think that everything is okay and that there is no cause for alarm (Hopkins, 2010). This factor inhibits most organisations from drawing an ISDRP.

Some enablers of ISDRP has been documented in the various IS literature. For instance, Choi and Johanson (2012) posits that a key driver for successful ISDRP is active support of senior management. This assertion is supported by Gopal and Gosain (2010) when they stated that management must have a greater stake in ISDRP. His argument was based on the notion that managers are those who have that strategic eyes and know where they intend to take the

organisation to and what they decide for the organisation is what stands. So, if ISDRP is made a strategic initiative it's definitely bound to materialize. The need for management support is essential and necessary as it is senior management that is ultimately accountable and charged with the task of initiating and supporting important projects with adequate funding and resources (Williams, 2011). The role of management in ISDRP cannot be over emphasized.

2.3.3 Implementation of ISDRP

This session refers to literature and research which discusses the implementation of ISDRP. Modern organisations have been said to be increasingly dependent on information technology (IT) and information systems (IS) to facilitate their businesses (Tiwana (2012). Research on the implementation of ISDRP are gradually increasing (Berente, Baxter, & Lyytinen, 2010; Majchrzak, Jarvenpaa, & Hollingshead, 2007; Berente, Baxter & Lyytinen, 2010). Researches demonstrates how communication networks like the internet exchange, share, and transmit information in real time between suppliers, vendors and buyers in an industry value chain to carry out business transactions (Boland, Lyytinen & Yoo, 2007). Within the manufacturing environment, computer-aided design technologies help the product development team capture more customer requirements and develop better products to meet their specific needs (Lee & Berente, 2012). These few examples demonstrate that IT/IS is being harnessed as a key enabler for an organisation's operations in the present network economy. Tiwana, Konsynski, & Bush (2010) indicated the importance of implementing ISDRP in organisations. The aforementioned importance and benefits an organisation derives from ISDRP will make it extremely difficult for them to carry out their business operations if their IS are struck by a disaster (Lee & Berente, 2012). Orlikowski (2007) stated therefore the benefits organisations stand to benefit by implementing an ISDRP.

The increased reliance on IS however, poses a potential threat for an organisation (Leonardi, 2011). This is because the occurrence of catastrophic events or disasters affects its IT/IS operations and causes their failures. Gregor & Jones (2007) adds that the organisation may suffer from the interruption of their supported business functions. As a consequence, the issue of how to strengthen IS capabilities so that a company can prevent or quickly recover from disasters becomes a serious concern (Slaughter & Kirsch, 2013). Clearly, an organisation depending on IS to support its business processes and functions needs to implement an effective ISDRP to ensure business continuity in the event of disaster strikes (King, 2013).

There exist a number of challenges that constrain ISDRP in organisations (King, 2008; Carr, 2008). For example, lack of allocated funds due to low priority for ISDRP (King, 2008) can inhibit a successful implementation of ISDRP. If planning against disaster is not on the priority list of organisations, it is of no doubt that much funds will not be allocated for it. Without sufficient and necessary funds a proper and effective DRP cannot be developed but even if it is developed it cannot secure or protect the necessary information it must if disaster strikes (Carr, 2008).

2.3.4 Evaluation of ISDRP

This session refers to literature and research which discusses the evaluation of ISDRP. Ramingwong and Sanjeev (2007) revealed that there are five elements of a successful ISDRP which falls into two categories of prevention and cure. These five elements are;

1. Business impact analysis
2. Secure offsite storage
3. Disaster management planning

4. Equipment replacement
5. A standby site.

Gopal and Gosain (2010) in contrast to Ramingwong and Sanjeev (2007), is of the opinion that the cure aspect of ISDRP should, if possible be prevented because the best type of disaster recovery plan is the one which is not implemented. To him proper and appropriate measures should be put in place in organisations to even prevent less to talk about cure after a disaster. What these studies perhaps did not do is to look at ISDRP from a more strategic perspective involving management.

Gopal and Gosain (2010) asserts that a typically disaster recovery (DR) backup strategies are organized into three data back-up site categories: cold, warm or hot sites. Cold sites are the least expensive to operate. The warm site offers a higher degree of sophistication and features an alternate location where data could be relocated after disruption. A hot site is the most expensive option; it offers full technological capacity to enable a seemingly fool-proof recovery process. Depending on how quick and cost effective an organisation wants develop an ISDRP; it can adopt any of the strategies. Bjornson and Dingsoyr (2008) also indicated that infrastructure complexity and investment cost are the two major issues to guide ascertaining the appropriate DR model. In the case of small and medium-sized businesses, the availability of technical resources and DR budget limitations are factors that dictate reasonable recovery spending (Williams, 2011), but can still yield effective benefits. Therefore, decisions related to allocating these resources are important to ensure that organisational sustainability is maintained. Bryson et al. (2002) states the importance of using mathematical models to analyze and design DR models. Prior model analysis indicates that the more physical components (hosts) in a DR infrastructure, the greater the probability of a hardware failure (Capgemini, 2011). While, additional hardware can provide a higher degree

of fault tolerance that hardware will also increase the DR expense from both the hardware and personnel perspective (Initiative, 2012).

2.4 Methodological Approaches and Issues in ISDRP research

This section categorizes and analyses the issues and methodological approaches taken in the review, providing the basis upon which gaps in methodology and issues are identified in the study. The table below positions each study according to the issues and methodological approach used.

Mapping of Articles Surveyed According to Issues and Methodological Approach Taken

Table 2.3

Method/Issue	Adoption	Development	Implementation	Evaluation
Quantitative	22	11	12	8
Mixed-methods	11	18	7	11
Qualitative	18	11	8	7
No defined methodological approach evident	11	9	6	4

Table 2.3 provides the categorization of issue adopted in the IS literature together with the methodology adopted in each study. For instance, in the adoption papers identified, 22 were quantitative, 11 used the mixed method while 18 used qualitative method. Eleven (11) of the adoption paper had no defined methodological approach evident.

Eleven (11) of the ISDRP development papers were quantitative, 18 used the mixed-methods and 11 also used the quantitative method. However, 9 of the IS development papers had no defined methodological approach evident. Furthermore, 12 of the ISDRP implementation papers identified used the quantitative method, 7 used the mixed-methods approach while 8

used the qualitative approach and seven (7) of the implementation papers also had no defined methodology approach. Additionally, among the ISDRP evaluation papers reviewed, 8 of the papers used the quantitative method, 11 of the papers used the mixed-methods while 7 of the papers used the qualitative method. However, just like the issues 4 of the ISDRP evaluation papers had no defined methodological approach evident.

2.4.1 Methodological Issues

Table 2.4

Method	No. of articles
Quantitative	53
Qualitative	44
Mixed method	47
No defined methodological approach evident	30

The number of studies employing a rigorous approach to methodology was also identified in the literature. Out of the 178 articles surveyed, 53 were quantitative, 47 used the mixed method, 44 used qualitative while 30 of the surveyed articles were purely descriptive and did not have any defined methodological approach evident. However, the absence of defined methods of enquiry did not necessarily detract from the insightfulness of the reported cases which were often informed by experienced practitioners or by those closely involved in ISDRP. Often, as in the case of Salger and Engels (2010) and Rottman (2008) the methodological approach, although not made transparent, was indicative of action research which can be a particularly appropriate method for investigating new phenomena.

Most of the articles made use of the quantitative method approach (Sedera & Gable, 2010; Ramchand & Pan, 2012) that use questionnaire survey techniques to extract individual or

organisational level data from samples of a few hundred respondents within a geographical spread confined to a particular district or region. Varying levels of reliability and validity testing have been built into most of the surveys, with the findings of some based on quasi-experimental design creating control groups of adopters and non-adopters ISDRP. Most studies lack triangulation either through use of multiple research methods to cross check data, or by comparing data from differing groups of stakeholders. The representativeness of the findings is open to question in a number of the studies with relatively small samples and lack of stratification and coverage. The level of analysis is predominantly micro carried out amongst individual IT/IS managers, rather than the whole organisation.

Detailed qualitative research is also high in the literature surveyed. Case studies drawing on primary evidence are provided by Goldoni and Olivia (2010) and Attarha and Modiri (2011). These provide valuable insights, but are representative of exploratory or work in progress, and overall, there is a noticeable lack of in-depth qualitative case studies that could provide a basis for theorizing.

Another issue linked to methodology concerns gauging the impartiality of the studies that are non-peer reviewed (Gefen & Carmel, 2008; George, 2010). Many of the key studies have been funded by industry research bodies. The orientation towards industry and organisational needs is reflected in the use of business and organisational survey techniques in many of the reports concerned. A number of studies, however, were carried out by external consultants that were independently funded by donors, and these seem to provide more scope for impartiality, a greater focus on social research indicators, and a greater degree of critical analysis.

2.4.2 Conceptual Approaches

Table 2.5 Distributions of Articles by Theoretical Frameworks

Theoretical Frameworks	Number of Articles
Group-1 Adoption of ISDRP	
Contingency model (Kovoor-Misra, 1995)	**7**
Protection motivation theory (Rogers, 1983)	**2**
Theory of planned behavior (Ajzen, 1991)	**2**
Group-2 Development of ISDRP	
Scale-free degree distribution theory (Boccaletti et. al., 2006)	**5**
Game- theoretic model (Neumann and Morgenstern, 1944)	**4**
Delone and McLean's model of IS success	**4**
Emergency management model (Richardson, 1994)	**7**
Group-3 Implementation of ISDRP	
A process modeling framework	**6**
Redundancy allocation model	**2**
Discrete optimization model	**1**
Business Process Management (BPM) framework (Harmon, 2010)	**3**
Knowledge work matrix (Davenport, 2005)	**1**
Group-4 Evaluation of ISDRP	
Viable system modeling (VSM)	**1**

With reference to Table 2.4, Group 1 consists of theoretical frameworks used in studying issues relating to the adoption of information systems disaster recovery planning. Contingency model is that most commonly used (7 articles). As a result, ISDRP research on adoption has a fundamental theoretical understanding that facilitates easier formulation of research models and their replication in research in different sectors or industries and makes the knowledge contributed more theoretically and practically grounded. Group 2 consists of theoretical frameworks used in studying issues relating to the development of ISDRP. Emergency management model tend to be the underpinning theory of quite a number of

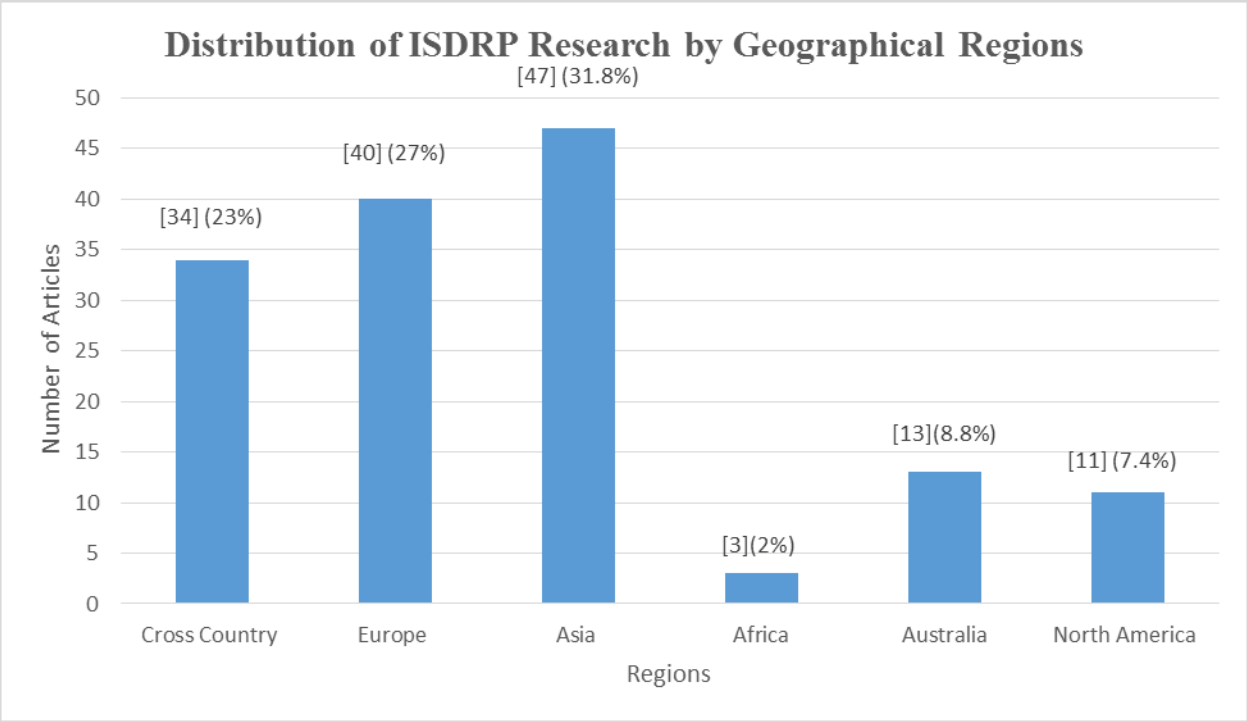
ISDRP papers relating to development. It comprised of (7 articles). Group 3 consists of theoretical frameworks used in studying issues relating to the implementation of ISDRP (Table 2.3). However, compared with Group 2, Group 3 tends to have no theory that has been widely used in theoretical models to study the implementation for ISDRP research. The dominant theoretical framework is the process modeling framework and the BPM framework. Further research employing these theories would therefore contribute substantial knowledge theoretically and practically in ISDRP. In Group 4 only one theoretical framework was found in the issues of evaluation of ISDRP. This was the viable system modeling (VSM). However, it is important to note that some of the Groups consist of publications that use models formulated from literature review with no specific or underpinning theory.

This research investigated information systems disaster recovery planning (ISDRP) by drawing upon two relevant theories i.e. the theory of planned behavior (TPB) and the protection motivation theory (PMT). Ifinedo (2011) used the aforementioned theories to investigate information system security compliance in an organisation which led to the proposal and validation of the aforementioned theories. Therefore drawing upon the theory of planned behavior (TPB) and the protection motivation theory (PMT) to investigate ISDRP is likely to generate interesting insights. Additionally, it is evident from table 2.3 that PMT and TPB have not been used much in IS researches. Therefore using them in this study will contribute significantly to literature. An in-depth explanation of the PMT and TPB is provided in the next chapter.

2.4.3 Geographical Issues

Geographical focus explores the geographical distribution of current research in ISDRP. The distribution on ISDRP literature reviewed in this study fairly indicates that most of the present literature (published in journals reviewed here) are concentrated in Asia (26.4%), and Europe (22.5%), the less represented regions are Africa (1.7%), Australia (7.3%) and North America (6.2%) as shown in Figure 2.3

Figure 2.3 Distribution of ISDRP Research by Geographical Regions



Within these regions differences do occur with respect to the number of articles per country. Thailand and India tend to dominate the ISDRP articles in Asia. Particularly for India, these articles tend to focus on adoption or the development of ISDRP (Klein and Rai 2009; Schubert and Legner, 2011). Literature on Thailand covers both development and evaluation of ISDRP. These studies include the first approach in the assessment of the complexity ISDRP models for SME's (Gopal and Gosain, 2010). Mete and Zabinsky (2010) argue that

organisations without a properly developed ISDRP will find it extremely difficult to resume its critical business functions if disaster should strike its IS.

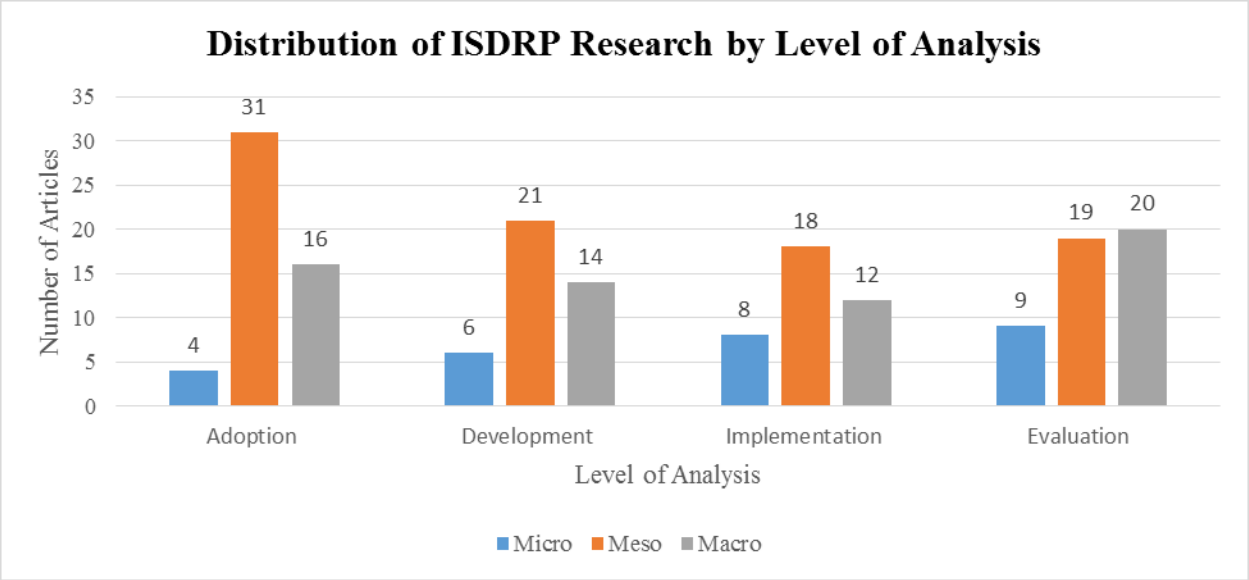
In Europe, the dominant countries in the literature are UK (Pollock & Williams, 2009) and Spain (Fabian and Dhillon, 2007). Pollock and Williams (2009) argue that for organisations in Europe to have the full benefit that comes with ISDRP, the planning should be made a strategic initiative. Thus management must have a giant stake in it before it can be successful. Their findings suggests that since DRP encompasses all aspects of the organisation, management should be made to understand what their organisation stands to get when DRP is inculcated in their operations so that they can make provision for that.

The least represented region with respect to the topic under review is Africa. Three papers were identified and South Africa tends to dominate the ISDRP articles in Africa (Kgakats & Rautenbach, 2013; Raju & Niekerk, 2013). Perhaps the reason for Africa being under researched may be the political instability within certain countries in the region, making it unattractive to researchers in the developed world, as previously experienced in Libya and Egypt's uprising. There is also the issue of poor collaboration of the private sector and the academics in tertiary institutions in Africa, which influences the potential for research. Moreover, these tertiary institutions may offer few programs within the IS discipline due to the lack of requisite human and technical resources to offer such programs. This relatively limits the space for substantial IS research. Even where such requisite resources exist, the political and financial constraints related to the funding of tertiary institutions in Africa affect the allocation of grants to support such research activities.

2.4.4 Level of Analysis

This category refers to the level of analysis employed or conducted in the research. Macro level studies cover comprehensive evaluation and case studies of ISDRP in countries. Meso level studies focus on ISDRP in a particular organisation. Whereas micro level studies refer to studies which focus on individual ISDRP.

Figure 2.4 **Distribution of ISDRP Research by level of Analysis.**



The distribution on ISDRP literature reviewed in this study fairly indicated that most of the present research has been conducted at the meso level or organisational level and macro level as shown in figure 2.4 above. The dominance of ISDRP literature on the meso level reveals the phases that topic has gone through or is going through. This finding reiterates earlier a finding in literature that IS has become an indispensable organisational asset (Farazmand, 2007) and that organisations may not be able to conduct business if there IS are malfunctioning. This may be the reason why the literature tends to focus more organisational level ISDRP.

2.4.5 Distribution of Articles by Year of Publication

Figure 2.5

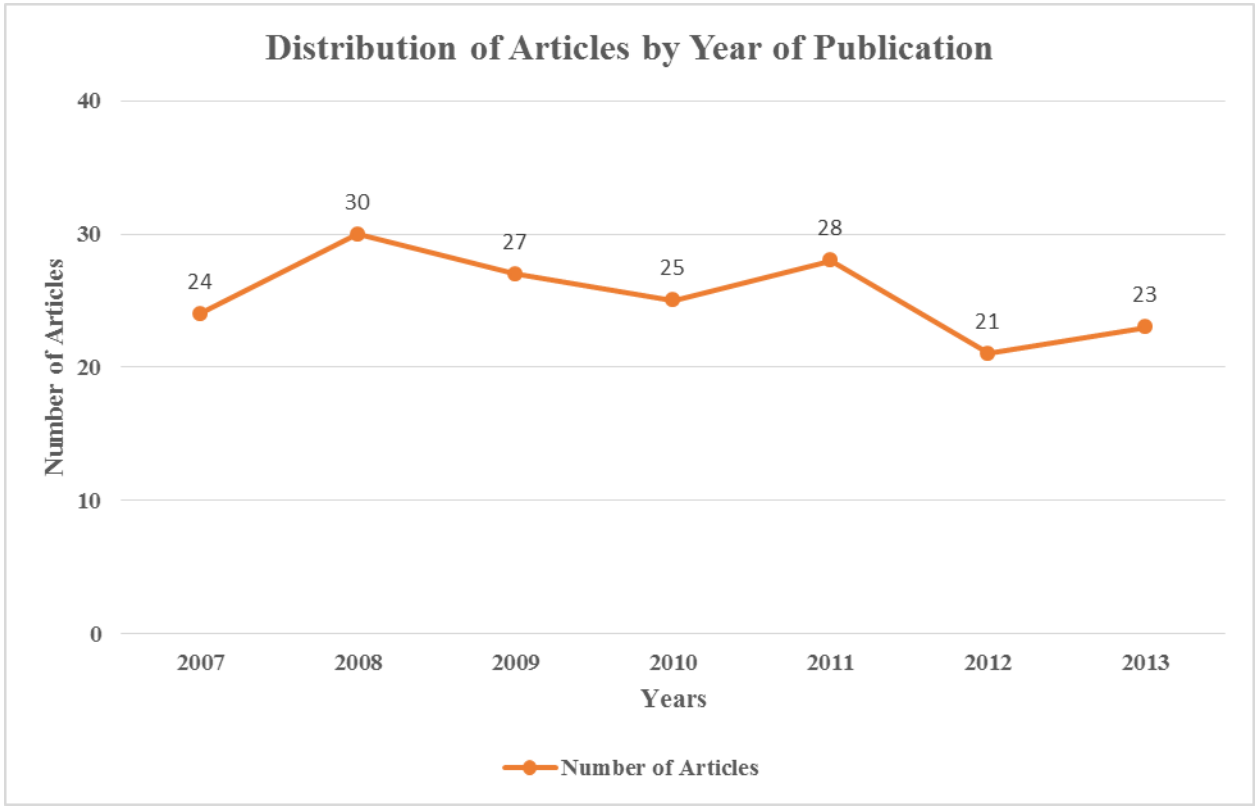


Figure 2.5 shows the distribution of articles by year from 2007 to 2013. It demonstrates an even distribution of the articles within the years under review. The highest number of articles was published in 2008, after which it declined to 27 and 25 in 2009 and 2010 respectively. 2011 saw an increase to 28 articles and dropped to 21 in 2012. The even distribution of the articles is a result IS journals publishing a number of articles on ISDRP. This is a result of the fact that IS has become an integral part of organisation and disaster on IS can be very costly for organisation, hence the need to enlighten and educate the people on ISDRP.

2.5 Factors that enable or constrains ISDRP

This session of the review focuses on the drivers and key inhibitors of information systems disaster recovery planning. A number of studies have conducted on this issue (Zu and Kaynak 2012; Basu and Lederer 2011). A summary of the drivers and inhibitors of ISDRP as reviewed from the literature is provided in the table below.

Table 2.6 ***Drivers and Inhibitors of ISDRP***

Drivers of ISDRP	**Inhibitors of ISDRP**
Active support of senior management (Choi and Johanson, 2012; Gopal and Gosain, 2010).	Lack of management awareness (Brynjolfsson and Schrage, 2009).
Commitment of funding (Aral and Weill, 2007; Mithas and Jones, 2007).	Lack of security awareness and training for all staff (Hopkins, 2010; Han and Mithas, 2011).
Protection of information assets (Bardhan, 2007).	Lack of allocated funds due to low priority (King, 2008; Carr, 2008).
Negative experience(s) can drive change (Kohli, 2007).	No negative experiences so it is assumed that everything is ok (Kohli, 2007).
Staff awareness and training (Mithas and Jones, 2007).	Lack of capacity / resources to test DRP (Gopal and Gosain, 2010).
Standards and legislation for vital records may be enforceable (Bardhan, 2007).	Lack of current and appropriate DRP processes (Brynjolfsson and Schrage, 2009).
DRP processes to encompass the whole organisation (so every employee must be involved) (Carr, 2008).	Expectation of users to be able to access all information when they want (Hopkins, 2010).

To start with, let's delve into the drivers of ISDRP as documented in the various IS literature. According to Choi and Johanson (2012) a key driver for successful ISDRP is active support of senior management. This assertion is supported by Gopal and Gosain (2010) when he

stated that management must have a greater stake in ISDRP. His argument was based on the notion that managers are those who have that strategic eyes and know where they intend to take the organisation to and what they decide for the organisation is what stands. So if ISDRP is made a strategic initiative it's definitely bound to materialize. The need for management support is essential and necessary as it is senior management that is ultimately accountable and charged with the task of initiating and supporting important projects with adequate funding and resources (Williams, 2011). The role of management in ISDRP cannot be over emphasized.

Another key enabler of ISDRP according to Aral and Weill (2007) is commitment of funding. Funding is a major factor that determines how far an organisation can realize or achieve its projects. Mithas and Jones (2007) posited that sufficient funding motivates workers and employees to give all their best knowing very well that their effort will result in a profitable outcome. If enough funds is allocated to ISDRP, there is a high tendency that the planning process will be effective and not be shawn along the way (Kohli, 2007).

The protection of critical business information is a driver for ISDRP (Bardhan, 2007). The greatest asset of an organisation is its assets. So for an organisation to have a competitive urge of its competitors its assets (information) and systems containing this information must be secured even in the midst of disaster (Bennett 2009). In order not to go down or halt business should a disaster strike, many organisations are putting in place strategic measures to resume their critical business functions if their information systems get struck by disaster (Feld 2009).

Kohli (2007) was also of the opinion that previous negative experience with disaster can be a driver for ISDRP. An organisation that have experienced a disaster will put in the right checks in place in order to minimize the effect of the disaster should it strike again (Im and Rai 2008).

2.5.1 Key inhibitors to a successful ISDRP

Just as several factors drives ISDRP, a number of factors can as well can stall/hamper organisations from successfully planning against disaster. Brynjolfsson and Schrage (2009) disclosed that lack of management awareness to the ISDRP can constrain the planning process. As indicated by Gordon and Tarafdar (2010) it is senior management that is ultimately accountable and charged with the task of initiating and supporting important projects with adequate funding and resources. So if managers are not made aware of ISDRP it is likely the plan would not materialize but even if it does it will not receive the necessary support it deserves.

Hopkins (2010) is of the opinion that lack of security awareness and training for all staff could be an inhibitor to a successful ISDRP. Training of staff on ISDRP is a very critical issue in organisations since the plan against disaster has to be designed and implemented by the staff of the organisation. Inadequate training of staff will lead to loop holes in the disaster recovery plan (Han and Mithas, 2011). Lack of security awareness can also hinder ISDRP in that the employees or managers will not see the reason why they should provide security for their information assets. All these without any doubt can be said to hinder a successful disaster recovery planning. And this can affect the operations of organisations.

Lack of allocated funds due to low priority for ISDRP (King, 2008) can also inhibit a successful ISDRP. If planning against disaster is not on the priority list of organisations, it is of no doubt that much funds will not be allocated for it. Without sufficient and necessary funds a proper and effective DRP cannot be developed but even if it is developed it cannot secure or protect the necessary information it must if disaster strikes (Carr 2008).

Furthermore, because organisations might not have experienced any disaster, they might think that everything is okay and that they is no cause for alarm (Hopkins, 2010). This factor could inhibit most organisations from drawing an ISDRP.

2.6 Research Gaps and Future Research Directions

This final section identifies key research trends and gaps relating to the issues and evidence and the theoretical and methodological approaches followed in the reviewed studies.

2.6.1 Gaps in Issues and Evidence

As indicated through the literature reviewed, there exists a plethora of research on the adoption and motivation for ISDRP (Klein and Rai, 2009; Mete and Zabinsky, 2010; Howden, 2009), far more than any of the issues that were identified in the reviewed literature. The lack of evidence concerning development, implementation and evaluation of ISDRP gives the relatively small number of articles in those domains of ISDRP. The small number of articles focusing on the development, implementation and evaluation of ISDRP, however, is a more significant research gap. A number of the articles reviewed also discussed more on ITDRP (Shroshpire and Kadlec, 2009) but it is well-established that IT is a component of IS. It is therefore expedient to look more into a much broader view of ISDRP of which IT is a component.

2.6.2 Gaps in Conceptual Approach

The main objective of this section is to offer a brief summary of a sample of relevant theories that could be used to gain a better understanding of the key aspects of DR process management in the field of IS. It is envisaged that better understanding of these aspects could possibly lead to their better management of ISDRP in the future. Table 2.3 provided a number of frameworks that has been used to study ISDRP. However, it is evident that some frameworks have been used severally in these studies an example is contingency model and the process modeling framework. While other frameworks like the protection motivation theory and the theory of planned behavior have been under used in ISDRP researches. There is therefore a call to use these theories to explore ISDRP since it may generate interesting insights. For this reason, the researcher adapted the theory of planned behavior and the protection motivation theory to study ISDRP among organisations in the Ghanaian banking sector.

2.7 Gaps in Methodological Approach

The most apparent gap in the use of methods was the lack of in-depth qualitative studies analyzing primary data in contrast to the loosely-positivist mixed-method approaches which tend to dominate the area of study. Lack of depth of qualitative data may explain lack of conceptualization as such studies have played an important role in other avenues of research concerning the application of ICTs to development (Walsham & Sahay, 2005). However, for the purpose of this study the quantitative approach would be used in order to answer the research questions and achieve the purpose of the study.

2.8 Conclusions and Pointers for Future Research

This review indicates a rapid expansion of research into IS/IT DRP, and as yet there has been little study on ISDRP using an in-depth qualitative study. This paper is intended to fill that gap by doing an in-depth qualitative coupled with quantitative analysis (mixed method) to improve their reliability through use of larger and more carefully constructed samples. It is hoped that the studies reported here are representative of the field of research, and the interpretation of those studies by the authors accurately reflects the research conducted.

Overall, the reviewed studies indicate

- Literature on issues concerning the adoption of ISDRP is relatively higher than other issues identified such as development, implementation and evaluation of ISDRP.
- Specific attempts to develop theoretical models, and create a deeper understanding of ISDRP, most noticeable in the area of ISDRP adoption.
- The most apparent gap in the use of methods was the lack of in-depth qualitative studies analyzing primary data in contrast to the loosely-positivist mixed-method approaches which tend to dominate the area of study. Lack of depth of qualitative data may explain lack of conceptualization as such studies have played an important role in other avenues of research concerning the application of ICTs to development (Walsham & Sahay, 2005).

In terms of pointers to future research, the following should be considered.

- Issues of ISDRP based on different geographical locations might generate interesting insights. For instance the approach organisations in the developed countries might take concerning ISDRP can be different from that of developing countries. This could

be due to culture and other environmental settings. IS researchers can research deeper into factors that might cause these disparities.

- Apart from the dominant theories that have been used to discuss ISDRP, researchers can explore the use of other theories like the actor-network theory, the boundary object theory, the boundary spanning theory and the theory of coordination to further discuss ISDRP. However, this research responds to some of the aforementioned gaps by addressing the enablers and inhibitors of information systems disaster recovery planning in the Ghanaian banking sector. This research also integrated the theory of planned behavior (TPB) and the protection motivation theory (PMT) as the theoretical lens to achieve the research purpose.

2.9 Summary

This chapter started with an introduction and the rationale for the review. It was followed by a session which highlighted the framing of the IS research. The methodology for the literature review was also discussed together with the issues, methodology and conceptual approaches discussed in ISDRP literature. Finally research gaps and future research directions were pointed out. However, this research responds to some of the aforementioned gaps by addressing the enablers and inhibitors of information systems disaster recovery planning in the Ghanaian banking sector. This research also integrated the theory of planned behavior (TPB) and the protection motivation theory (PMT) as the theoretical lens to achieve the research purpose.

CHAPTER THREE

CONTEXT OF THE STUDY

3.1 Introduction

This chapter provides a synopsis of the context on which this study is based, that is the banking industry or sector in Ghana.

3.2 Brief overview of the banking sector in Ghana

The banking sector is the backbone of the Ghanaian economy and plays an important financial intermediary role; therefore, its health is very critical to the general economy at large. At the time of this research, the banking sector of Ghana comprises 28 banks. Currently, all banks in Ghana are operating as universal banks with almost limitless range of products. The banking sector has seen the arrival of many banks from the sub-region as it is the policy of the central bank to encourage international banks with repute to operate in Ghana. The policy is geared toward supporting the development of a well-capitalized and robust financial system (Price Waterhouse Coopers, 2008). The traditional core business of banks in Ghana has been retail and corporate banking.

The bank of Ghana (BoG) has introduced the Ghana Interbank payment and settlement system enabling common electronic platform for the across financial institution (Bank of Ghana, 2008). One such platform is the National Switch and Smartcard Payment system dubbed ‘Ezwich’ and cheques Codelines Clearing with Cheque Truncation System to replace the existing manual (paper-based) clearing system.

The banks in Ghana are offering a wide range of products and services for customers. These include prestige banking, cash passport, executive loans, child account, telephone banking,

electronic banks, internet banking, Automated Teller Machine (ATM) and transaction alert which hitherto was offered by a few banks but are gradually becoming a basic service across banks. Many products and services are now matters of competitive necessity rather than a competitive advantage (Willian et al., 2005).

In Ghana, there have been attempts to ensure efficiency and competitiveness in the banking industry. Among these initiatives were the movement to universal banking, adoption of an open licensing system, and the modernization of the payment system, including establishing a central securities depository and the passage of supportive laws. Universal banking, which involves the removal of restrictions on the banking activities, was introduced to allow banks to choose the type of banking services they would like to offer in line with their capital, risk appetite, and business orientation. The purpose of this was to remove the monopoly that was given to commercial banks in the area of retail banking, and create room for diversification of the range of financial that a bank can provide. In addition it allowed merchant banks for example to compete for deposits. According to the central banks, this process should lead to branch network expansion, increasing banking penetration, and also competition for deposits at the retail level. Indeed, the movement into universal banking also came with a higher capital requirement to ensure that banks are sufficiently capitalized to take on additional risk (Acquah, 2006).

3.3 Information systems disaster recovery planning in the Ghanaian banking sector

The Ghanaian banking sector has played a significant role in poverty reduction, and it also has the potential for strengthening the risk management capacity of the poor. Access to banking services increases poor households' prospects of evading poverty and at minimum, falling further down the poverty line.

Provision of banking services that can have a sustainable impact on client's well-being and reduced vulnerability is not an easy endeavour; however the Ghanaian banking institutions face many risks that can adversely affect their long-term operational and financial sustainability. Some of the most serious risks pertain to the external environment in which these institutions operate, and include natural disasters, economic crisis and civil conflicts. Hence Ghanaian banks have to incorporate internal and external preparedness measures. Information systems disaster preparedness within the banking sector is of two-fold:

Internal preparedness. Capacity building of staff in the Ghanaian banking sector for preparedness is perhaps the most important task. Banks are unique in their way of operation as the staff has rapport with even the most remote clients. In the event of an emergency, banks personals are often the first to react to the disaster. Hence, they should be trained on IS disaster risk reduction before disaster.

External disaster preparedness. The Ghanaian banks can develop relationships with specialized institutions on information system disaster management. Except in areas frequently hit by cyclical disasters, banks are rarely aware of disaster warning systems. Rather than suggest that each bank creates these partnerships, however, the Ghanaian banking network may be more cost efficient channels to track and disseminate disaster warning information. All of these partnerships offer important opportunities for Ghanaian banks to become better prepared to serve their clients as well as survive the crisis themselves without losing their financial services perspective.

In Ghana, there are about 28 commercial banks operating a wide range of financial services. Some of these banks in Ghana and the services they provide are discussed below.

3.4 Agricultural Development Bank of Ghana

Agricultural Development Bank of Ghana, commonly known as Agricultural Development Bank or ADB, is a government-owned development and commercial bank in Ghana. The bank is the first development finance institution established by the Government of Ghana. It is one of the commercial banks licensed by the Bank of Ghana, the national banking regulator. ADB was established in 1965, by Act of Parliament to meet the banking needs of the Ghanaian agricultural sector in a profitable manner (www.agricbank.com). Before its current name, the bank was known as the Agricultural Credit and Co-operative Bank. The bank changed its name in 1970, when the parliamentary statute was amended to grant the institution full commercial banking powers. The Bank is a large development and commercial bank (www.agricbank.com). As of April 2010, ADB was the leading financial institution in agricultural financing in Ghana, responsible for 35% of the total bank industry financing of agriculture. In September 2010, the bank was recognized as *Bank of the Year* at the Africa Investor Agribusiness Awards, in Durban, South Africa, the first institution so recognized, at this annual event. The total assets of the institution at the end of December 2011 were valued at approximately US$683.6 million (GHS: 1.21 billion). In order to mitigate risk and maximize profits, the bank also engages in other types of banking beyond making agricultural loans. The range of services offered include: (a) Development Banking (b) Corporate Banking (c) Personal Banking (d) International Banking (e) Diaspora Banking Services (f) Treasury Management Services and (g) Money Transfer Services, in partnership with Western Union. The Bank maintains a network of fifty (78) branches located in all areas of Ghana. There are also an additional four (4) Farm Loan Offices and ten (ten) Agency Offices. This adds up to a total of sixty-four (64) service outlets, in addition to the bank's headquarters in Accra, Ghana's capital and largest city. At the time of this research, the

chairman of the board of the ADB was Alhaji Ibrahim Adam and the Managing Director is Stephen Kpordzih.

3.5 Cal bank

CAL Bank is a commercial bank in Ghana involved primarily in meeting the banking needs of small, medium and large corporations. It is one of the commercial banks licensed by the Bank of Ghana, the national banking regulator. Founded in 1990, CAL Bank is rated as "one of the most innovative banks in Ghana", according to its website. As of December 2010, the bank's total assets were valued at about US$266 million (GHS:510 million), with shareholders' equity of approximately US$41 million (GHS:79 million). The stock of CAL Bank is traded on the Ghana Stock Exchange under the symbol CAL. CAL Bank is headquartered in Accra, at 23 Independence Avenue. As at the time of this study, the bank operated fifteen (19) networked branches.

3.6 Standard Chartered

Standard Chartered Bank is a market – leading financial services brand in Ghana and listed on the Ghana Stock Exchange. It has operated since 1896 in the country and is among the consistent performing stocks on the exchange. It ranks among the top 20 companies in the 'Ghana Club 100' rankings by the Ghana Investment Promotion Centre (GIPC). The Bank's focus and commitment to developing deep relationships with clients and customers, through its Wholesale and Consumer banking business, has driven its consistent growth in recent years.

With a network of 24 branches and 52 ATMs across Ghana, Standard Chartered offers exciting product propositions for customers and clients as well as career opportunities for

over 1,000 employees in Ghana. It is committed to building a sustainable business over the long term in Ghana and is trusted worldwide for upholding high standards of corporate governance, social responsibility, environmental protection and employee diversity. The Bank's heritage and values are expressed in its brand promise – Here for good.

Corporate and institutional banking services are provided in three main locations in Accra (covering Tema, Kumasi and Takoradi). The currency of Ghana is the Cedi (SWIFT Code GHC), which is allowed to float against all currencies.

3.7. Review of Operations

3.7.1 *Consumer Banking*

Standard Chartered Bank Ghana offers a wide range of personal banking products and services nationwide through a network of 21 branches, 1 main Priority Centre at Opeibea with adjoining Priority Lounges at all our branches to cater for our Priority customers, 1 agency on the Kwame Nkrumah University of Science And Technology Campus and alternate channels such as ATMs, call centres, transactional banking, debit cards, personal loans, and SMS banking. Standard Chartered Bank is the only bank which has 2 SME centres in the country.

Customers enjoy the privilege of a banking partner that is flexible and tailors solutions to take care of their specific banking needs. Standard Chartered services are backed by a strong commitment to providing its customers with effective and reliable banking services and out serving their expectations.

3.7.2 Wholesale Banking

The wholesale banking of standard chartered provides innovative solutions to address the needs of valued customers. An extensive knowledge of international markets combined with a deep local insight puts the Bank in a unique position to provide quality advice and information on currencies, interest rates and risk management. The Bank has always been at the forefront of creative product offerings. Products offered include foreign exchange forwards and spots, high-yield deposits and foreign currency options. The Bank is an authorized Foreign Exchange Dealer of the Central Bank.

3.8 Summary

This chapter represented the context of the study. The profile of the organisations which responded to the survey questionnaire and interviews were presented in this chapter.

CHAPTER FOUR

RESEARCH FRAMEWORK

4.1 Introduction

The research adopts of the tenets of the Protection Motivation Theory (PMT) and the theory of planned behavior (TPB) to study the phenomena. The two theories; the theory of planned behavior (Ajzen, 1991) and the protection motivation theory (Rogers, 1983) will be integrated to increase our knowledge of ISDRP by employees and managers in modern organisations. Previous works have used research frameworks that integrated PMT and TPB with other theories (Herath and Rao, 2009; Lee and Kozar, 2005; Lee and Larsen, 2009). To the best of knowledge, no prior research has used both theories in a single study. Anderson and Agarwal's (2010) review of the literature in this area indicated that the two foregoing theories have been used by IS security research. This justifies the use of these theories in this research.

4.2 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, and

(d) Response efficacy, i.e., the ability of the response to reduce the threat (Maddux & Rogers, 1983; Rogers, 1983).

(e) Response cost, this factor emphasizes the perceived opportunity costs in terms of monetary, time, effort expended in adopting the recommended behavior.

Protection Motivation Theory (PMT), which developed by Rogers (1983) expanded the health-related belief model in the social psychology and health domains (Rippetoe and Rogers, 1987). Drawing from the expectancy-value theories and the cognitive processing theories, PMT was developed to help clarify fear appeals. PMT has been noted as one of the most powerful explanatory theories for predicting an individual's intention to engage in protective actions (Anderson and Agarwal, 2010). In essence, protection motivation emanates from both the threat appraisal and the coping appraisal. Threat appraisal describes an individual's assessment of the level of danger posed by a threatening event (Rogers, 1983; Woon et al., 2005). It is composed of the following two items:

I. Perceived vulnerability, i.e. an individual's assessment of the probability of threatening events.
II. Perceived severity, i.e. the severity of the consequences of the event.

The coping appraisal aspect of PMT refers to an individual's assessment of his or her ability to cope with and avert the potential loss or damage arising from the threat (Woon et al., 2005). Coping appraisals are made up of three sub constituents:

I. Self-efficacy - this factor emphasizes the individual's ability or judgment regarding his or her capabilities to cope with or perform the recommended behavior.
II. Response efficacy - this factor relates to the belief about the perceived benefits of the action taken by the individual (Rogers, 1983).
III. Response cost - this factor emphasizes the perceived opportunity costs in terms of monetary, time, effort expended in adopting the recommended behaviour.

The protection motivation theory has been used in quite a number of information systems research. For example, Ifinedo (2012) used the PMT to understand information systems security policy (ISSP) compliance. Following the constructs of the theory, he was able to define what goes into each of the variable. For instance, perceived vulnerability is an individual's assessment of the probability of threatening events; his study measured perceived vulnerability as the threat resulting from noncompliance with ISSP. Also, perceived severity was also measured as the imminent threats to the security of one's organisation's information arising from noncompliance with ISSP. Ifinedo (2012) measured self-efficacy as the sorts of skills and measures needed to protect the information in one's organisational information systems. Response efficacy referred to the compliance with ISSP as being an effective mechanism for detecting a threat to one's organisational IS assets. Thus, the perceived benefit of the action taken by the individual. Last but not the least the response cost emphasized the perceived opportunity costs in terms of monetary, time, effort expended in adopting the recommended behavior, in this instance complying ISSP. Their measurements proved that all the above explained variables affect positively the intention for ISSP compliance.

Furthermore, Vance, Siponen and Pahnila (2012) also adopted the tenets of the protection motivation theory to study the motivation of IS security compliance. To the authors, vulnerability is the probability that an unwanted incident will happen if no actions are taken to prevent it. In their study, vulnerability denotes employees' assessment of whether their organisation is open to IS security threats if no measures are taken to prevent them. Furthermore, in their context perceived severity refers to the severity of the IS security breach, and the possible negative event caused by the breach in an organisation. Hence they hypothesized:

H1. Vulnerability positively affects employees' intention to comply with IS security policies.

H2. Perceived severity positively affects employees' intention to comply with IS security policies.

PMT also consists of coping appraisal factors, which depend on the increase of the adaptive response. In their context, compliance with IS security policies should be an effective protection against IS security threats. Self-efficacy in their study, refers to employees' belief that they can successfully comply with IS security policies, which should enhance compliance with policies and procedures (Anderson and Agarwal, 2010). Finally, response cost includes the inconvenience incurred in complying with IS security policies. Hence they hypothesized:

H4. Response efficacy positively affects employees' intention to comply with IS security policies.

H5. Self-efficacy positively affects employees' intention to comply with IS security policies.

H6. Response cost negatively affects employees' intention to comply with IS security policies.

The results off their theoretical model analysis revealed that vulnerability had an insignificant effect on intention to comply. In contrast, perceived severity positively affected intention. Also, self-efficacy had a positive impact on employees' intention to comply with IS security policies (Woon et al., 2005). Furthermore, response cost negatively influenced employees' intention to comply with IS security policies, meaning that employees consider the inconvenience of adhering to IS security policies a legitimate reason for not complying with those policies. In addition response efficacy had a significant negative effect on intention to comply

According to the PMT, protection motivation is operationalized in terms of the "intentions" of the stakeholders to perform a recommended precautionary behavior and the intentions are influenced by the two sub processes of threat appraisal and coping appraisal (Maddux & Rogers, 1983; Rogers, 1983; Milne, Orbell, & Sheeran, 2002). The threat appraisal involves an appraisal of the severity of the threat and the stakeholder's vulnerability to the threat (Maddux & Rogers, 1983; Rogers, 1983). In threat appraisal, the variables used are perceived vulnerability, perceived severity and fear arousal (Maddux & Rogers, 1983; Rogers, 1983; Milne, Orbell, & Sheeran, 2002). The coping appraisal involves an appraisal of the stakeholder's self-efficacy and the response efficacy (Maddux & Rogers, 1983; Rogers, 1983). The variables used in coping appraisal are beliefs about response efficacy, self-efficacy, and response costs (Maddux & Rogers, 1983; Rogers, 1983; Milne, Orbell, & Sheeran, 2002). When an individual believes that the response will be effective and is confident of performing the recommended behavior and perceives the cost of disaster recovery exercise to be low, then he/she will be more likely to adopt the recommended coping response (Milne, Orbell, & Sheeran, 2002). Therefore, the protection motivation theory can be applied to study the motivating factors that influence organisations to implement disaster recovery planning.

4.3 Theory of Planned Behavior

Theory of Planned Behavior (TPB) was proposed by Ajzen (1991). It postulates that individual behavior is influenced by attitude, subjective norms, and perceived behavioral control. TPB is one of the most predictive persuasion theories, and has been widely used across differing domains. Prior body of knowledge has confirmed that an individual's intention to perform a behavior which in this research is the intention to develop an ISDRP is strongly influenced by the following variables: attitude, subjective norms, and perceived

behavioral control (Venkatesh et al., 2003; Bulgurcu et al., 2010). The three constituents of TPB as used in this current research are describes as follows:

(i) Attitude is defined as the individual's positive or negative feelings toward engaging in a specified behavior. In this study, it encapsulates attitude toward developing an information system disaster recovery plan in the Ghanaian banking sector by managers (Pahnila et al., 2007).

(ii) Subjective norms describe an individual's perception of what people important to them think about a given behavior. In this study, subjective norms refers to external factor that affects the managers in the banking sector's intention to develop an ISDR plan.

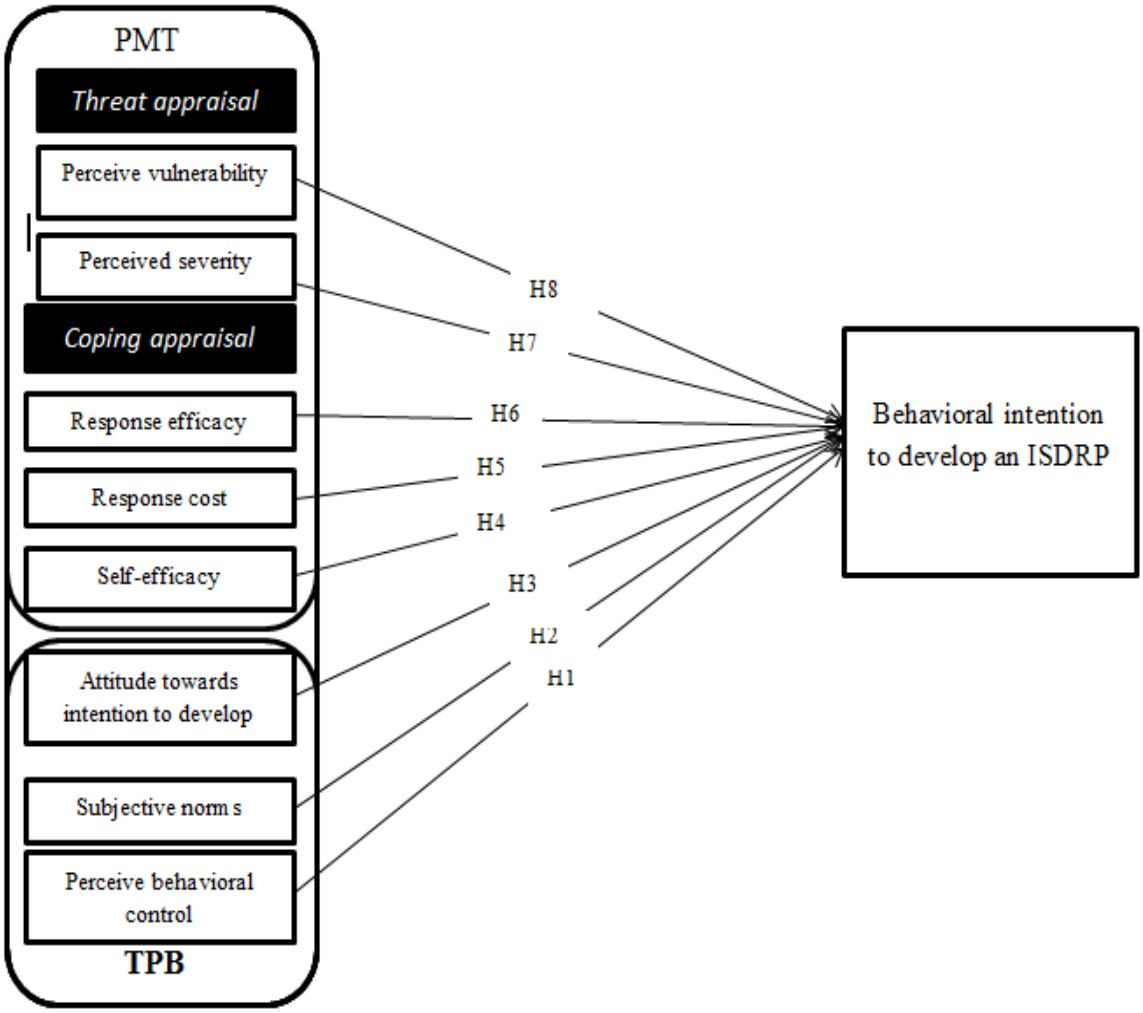
(iii) Perceived behavioral control, the third component of TPB was influenced by Bandura's (1991) self-efficacy in the social cognitive theory; it refers to an individual's perceived ease or difficulty of performing or facilitating a particular behavior.

TPB has been widely used in investigating information system's ethical behaviors and individual's decision to adopt acceptable computer security measures and comply with ISSP(Lee and Kozar, 2005; Leonard et al., 2004).

4.4 Research model and hypothesis

Following the preceding discussion, the research model is presented in Fig. 4.1.

Fig. 4.1 - integration of the theory of planned behavior and the protection motivation theory



Souce: Author's Construct

4.5 Operationalization of the research framework

This session of the chapter operationalizes the research framework to reflect the context in which it is being applied. This will give a better understanding of the research framework and how it applied to achieve the research purpose. This is illustrated in Fig 3.2.

Fig 4.2

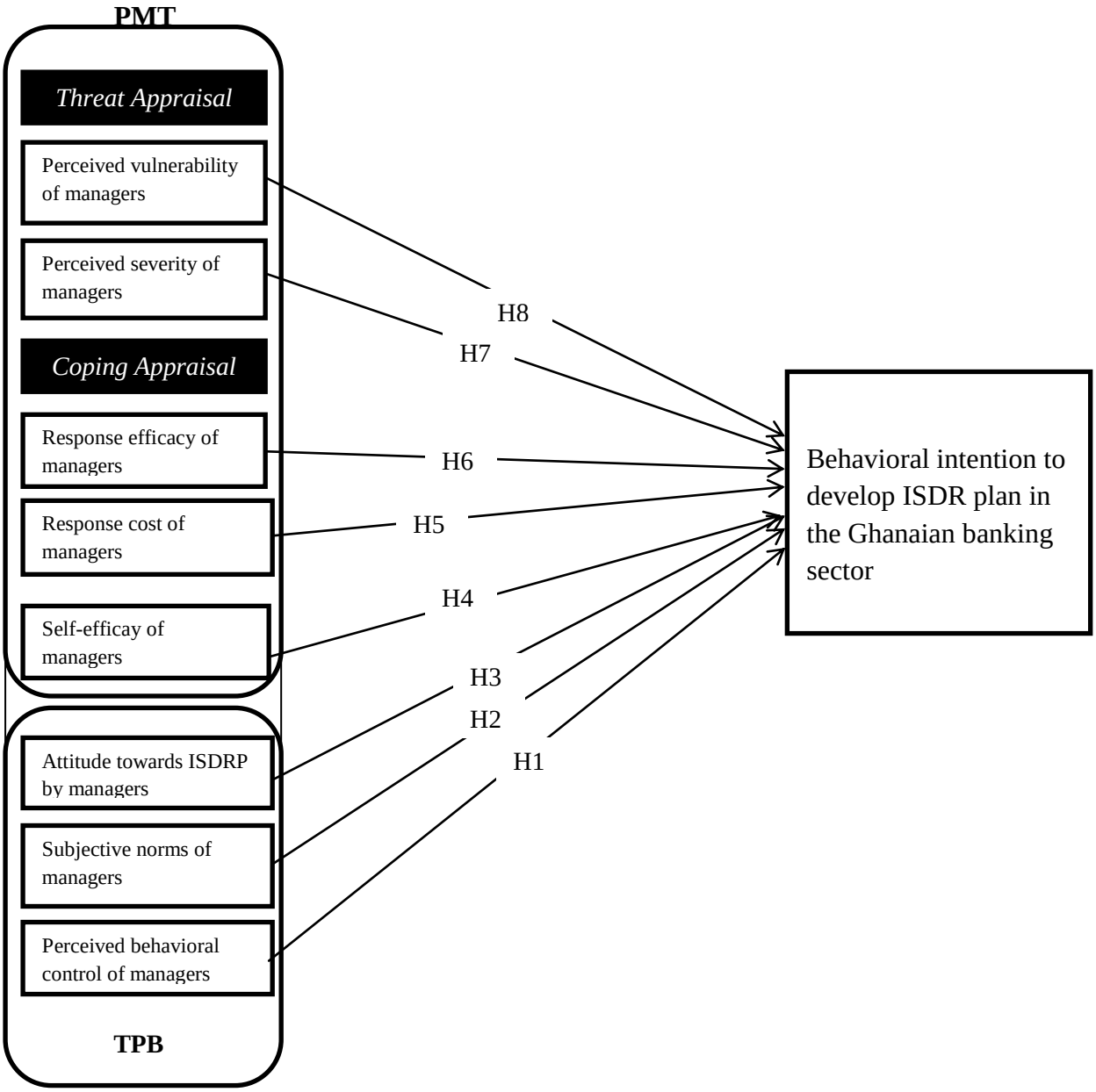


Fig 4.2 Conceptual Framework on the factors which influence managerial intention to develop ISDRP. (Adapted From Ifinedo, 2012)

Discussions on the research hypotheses are presented next.

Perceived behavioral control is defined as "the perceived ease or difficulty of performing the behavior" (Ajzen 1991, p. 188). In the context of IS research, perceived behavioral control is

defined as "perceptions of internal and external constraints on behavior" (Taylor and Todd 1995, p. 149).

Hypothesis 1 Perceived behavioral control (PBC) of managers will have an influence on the intention to develop an information systems disaster recovery plan in the Ghanaian banking sector.

Subjective norms are normative stimuli, beliefs and motivations to comply with a particular act, which is largely informed by consultation or observation of the behaviors of others (Ajzen, 1991; Aronson et al., 2010). It has been shown that an individual's behavior is influenced or motivated by what he or she observes to be the norm in his or her environment (Chan et al., 2005; Knapp and Marshall, 2006; Jonhston and Warkentin, 2010). In the context of ISDRP in organisations, employees are most likely to comply with their organisation's ISDRP if they notice that those around them, i.e. superiors, peers, and subordinates are complying with and abiding by such guidelines (Chan et al., 2005). The studies by Lee and Larsen (2009), and Herath and Rao (2009) found that subjective norms significantly affect information systems security policy compliance in organisations. Hence subjective norms can significantly affect the development of ISDRP in organisations.

Hypothesis 2 Subjective norms (SN) of managers will have an influence on the intention on the intention to develop an information systems disaster recovery plan in the Ghanaian banking sector.

The relationship between attitude and behavioral intentions has been widely tested in the IS literature (Venkatesh et al., 2003). TPB indicates that individuals' attitudes impact behavioral intentions (Ajzen, 1991). To that end, positive attitude toward ISDRP compliance indicates

positive behavioral intention for ISDRP. Conversely, negative attitudes will diminish an individual's intention to comply with the organisation's ISDRP. Thus, individuals with positive beliefs and values about their organisation's ISDRP will have favorable tendencies to comply with such rules, requirements, and guidelines (Herath and Rao, 2009; Bulgurcu et al., 2010). On the other hand, those lacking such favorable attitudes will not readily comply with such policies (Pahnila et al., 2007). Previous studies have shown that an attitude toward complying with acceptable IS behaviors positively impact behavioral intentions (Bulgurcu et al., 2010; Herath and Rao, 2009)

Hypothesis 3 Attitude toward ISDRP compliance of managers will have an influence on intention to develop an information systems disaster recovery plan in the Ghanaian banking sector.

As indicated above, self-efficacy emphasizes the individual's capabilities and competence to cope with the task or make a choice (Bandura, 1977, 1991). Self-efficacy has been shown to have a significant impact on an individual's ability to accomplish task behavior, including IS usage (Compeau and Higgins, 1995). In fact, Compeau and Higgins (1995) showed that people with higher levels of self-efficacy regarding IS use will employ such systems in their work more than those with low self-efficacy. With respect to ISDRP, it is to be expected that individuals with high IS security capabilities and competence will appreciate the need to follow organisational ISDRP and such individuals may be better placed to realize the threats of non- compliance.

Hypothesis 4 Self-efficacy (SE) of managers will have an influence on the intention to develop an information systems disaster recovery plan in the Ghanaian banking sector.

According to Pahnila et al. (2007), response costs may include monetary expense, timing inconveniences, embarrassment or other negative consequences, which result from an individual's behavior. Workman et al. (2008) commented that "people maintain different cost/benefit attitudes about information security measures that are independent of the perceived business value or sensitivity of the informational assets (i.e., severity of threat), particularly in relation to their own self-interests." Thus, individuals are reticent to follow or adopt recommended responses if they perceive that a considerable amount of resource i.e. time, effort, and money will be expended toward an effort (Lee and Larsen, 2009). Conversely, if small amounts of resources are required in implementing a measure, it may be adopted (Pechmann et al., 2003; Workman et al., 2008). Reducing the response cost tends to increase the likelihood of an individual performing a recommended behavior (Woon et al., 2005). Past studies have shown confirmed that response costs is negatively related to intention to use security measures.

Hypothesis 5 Response cost (RC) of managers will have an influence on the intention to develop an information systems disaster recovery plan in the Ghanaian banking sector.

When an individual possesses requisite knowledge about the effectiveness of a recommended coping mechanism in providing protection from a threat or danger, the individual is more likely to adopt an adaptive behavior (Rogers, 1983; Lee and Larsen, 2009). On the other hand, if the individual has less belief regarding the effectiveness of a measure, he or she may not readily accept it (Rippetoe and Rogers, 1987). Accordingly, individuals who believes that their organisation's ISDRP as guidelines and coping mechanisms to avert threats and dangers in their context will more likely to develop an intention to develop it (Herath and Rao, 2009).

Hypothesis 6 Response efficacy (RE) of managers will have an influence on the intention to develop an information systems disaster recovery plan in the Ghanaian banking sector.

In general, when individuals perceive a threat, they often adjust their behaviors in response to the amount of risk and determine if they are willing to accept the threat or not (Milne et al., 2000; Workman et al., 2008). Thus, an individual's perceived severity tends to be positively linked to their intentions to follow protective actions (Pechmann et al., 2003). If an individual perceives a threat (disaster) to his or her organisation's IS assets, such an individual will more likely follow guidelines and requirements laid out in their ISDRP (Bulgurcu et al., 2010; Pahnila et al., 2007). On the other hand, if an individual does not perceive a threat in his or her contexts vis-a-vis using organisational IS resource, he or she may be less concerned about adhering to directives provided in their ISDRP. The study by Herath and Rao (2009) found that perceived severity has a significant effect on intention to adopt ISSP by employees.

Hypothesis 7 Perceived severities (PS) of managers will have an influence on the intention to develop an information systems disaster recovery plan in the Ghanaian banking sector.

With respect to safe operation in the organisation, individuals who are of the view that they are invulnerable to security threats are more likely not adhere security measures at work (Herath and Rao, 2009; Bulgurcu et al., 2010). On the other hand, it is reasonable to expect that an individual who perceives high vulnerability to their organisations IS resource will be more likely to adopt protective behaviors. Lee and Larsen (2009) showed that perceived vulnerability has significant impact on business executives' intention to adopt security tools in their organisations.

Hypothesis 8 Perceived vulnerability (PV) of managers will have an influence on the intention to develop an information systems disaster recovery plan in the Ghanaian banking sector.

4.6 Summary

This chapter discussed the theories that were used for the research. The constructs and the variables were also discussed. The constructs for the two theories used in this study thus the protection motivation theory and the theory of planned behavior were explained and how they will be measured in this study. The hypotheses to be tested were enumerated and finally a diagrammatic representation of the framework was provided.

CHAPTER FIVE

METHODOLOGY

5.1 Introduction

In the previous chapter the research framework of this study was discussed. This chapter highlights the methodology adopted for the study. It consists of research paradigm, research design, research approach, sample size, data collection method, data analysis techniques, ethical considerations, research limitations and challenges.

5.2 Research Paradigm

This study was undertaken from the perspective of realism. The realism paradigm provides the information systems' researcher with both elements of positivism and constructivism (Healy & Perry, 2000). While positivism concerns a single, concrete reality and constructivism multiple realities, realism enables the IS researcher to acquire multiple perceptions about a single, mind-independent reality (Bisman, 2002). This study in extending the use of realism in IS research, gains the opportunity of obtaining detailed answers to the question of the factors that enable or constrain information systems disaster recovery planning in the Ghanaian banking sector. Thus examining the role managers play in developing ISDRP. Realism recognizes that perceptions have certain plasticity (Churchland, 1979) and that there are differences between reality and people's perceptions of reality (Bisman, 2002). Rather than being supposedly value-free, as in positive research, or value-laden as in interpretive research (Lincoln & Guba, 1985). Table 4.1 below shows the philosophical assumptions in realism and how they apply to my work.

Table 5.1

Philosophical assumptions	**Realism**	**Application of realism in this study**
Ontology	Objective reality is distorted by human subjectivity. Value cognizant; conscious of the values of human systems and of researchers.	In this research, the single, mind independent reality is ISDRP however; people including organisations have multiple perceptions about ISDRP. Hence the realist researcher investigated what the single reality of ISDRP is and what people actually perceive to be ISDRP.
Epistemology	The researcher is not entirely independent from what is being investigated. The knower and the known are co-created during the enquiry.	This was reflected in the study when the realist researcher went beyond what the reality of ISDRP is to know people's perceptions of the reality (ISDRP).
Methodology	Both qualitative and quantitative methodologies are seen as appropriate for researching the underlying mechanisms that drive actions.	In this study both qualitative and quantitative techniques were used to explore ISDRP in the Ghanaian banking sector.

However, the pending question is how does realism facilitate such an investigate exercise? To do this, the realist researcher observes the empirical domain to discover by a "mixture of theoretical reasoning and experimentation" (Outhwaite, 1983, p. 332) knowledge of the real world (in this research "an organisation"), by naming and describing the generative mechanisms that operate in the organisation and result in the events that may be observed. In this study, for instance, I combined both theoretical frameworks with other data collection

mechanisms in order to ascertain knowledge on the factors that enable or inhibits their ISDR planning in the Ghanaian banking sector. The realist researcher recognizes that perceptions about disaster are divergent (Churchland, 1979) and that there are differences between disaster and people's perceptions of disaster (Bisman, 2002). In this research, the single, mind independent reality is ISDR planning however; people including organisations have multiple perceptions about ISDR planning. It is now evident to the researcher that objective reality is distorted by human subjectivity. The researcher therefore needs to select appropriate data collection methods which fit the research paradigm and support the research purpose.

5.3 Research Design and Methods

A realist researcher who needs to investigate a phenomenon finds himself thinking about issues such as why it is necessary to study the phenomenon; the kind of knowledge it stands to develop; what the best way to gain knowledge is, and who will derive the benefits from the study (Harnesk, 2004). For the realist, exploratory research is one of the valuable medium to delve into ISDRP, seek new insights and to assess phenomena in a new light (Robson, 1993). Saunders, Lewis and Thornhill (2000) add that exploratory studies are particularly useful approach when a researcher wishes to improve a problem understanding. However because the objective of this study is to improve the understanding of ISDR planning in the Ghanaian banking sector, exploratory research is suitable. The realist researcher achieves this by gathering information on the multiple perceptions people (organisations) have, concerning ISDR planning. This provides the realist with the actual perception managers have regarding ISDRP.

Within a realism framework, both qualitative and quantitative methodologies are seen as appropriate (Healy & Perry, 2000) for researching the underlying mechanisms that drive

actions and events. The researcher therefore adopted the quantitative methods for this research. According to Creswell (2009) "survey provides a quantitative or numeric description of trends, attitudes, or opinions of a population by studying a sample of the population", for the purpose if this study, the target population is the Ghanaian banking sector. Hence, from the results of the sample, the researcher can then make claim or generalize about the population. Zikmund (2003) view a descriptive study as that in which there is previous knowledge about the phenomenon and its characteristics.

5.4 Conducting the Survey

5.4.1 Selection of sample for the Survey

According to Castillo (2009), samples are drawn because it will be impractical to investigate all members of a target population. Sampling is a process of selecting research participants (Creswell, 2009). To arrive at the sample or target population for this study, data collection was therefore scheduled in two stages consisting of a pilot study, which took place from 5th December 2013 to 12th January 2014 and a main study which took place from 18th January 2014 to 20th February 2014. In the pilot study, data (questionnaires) were collected across 18 different Ghanaian banking institutions. The firms selected were obtained from The Ghana Club 100 (GC100). The criteria for selection were related to my theoretical concepts, namely:

- Firms that adopt and employ information systems over a period of time and benefited from the use of information systems
- Firms with a historical account of developing information systems disaster recovery plan.

After the pilot survey seven of the organisations were willing to continue with the actual data collection. The rest of the organisations backed out because the information to be provided

according to them will touch on their private or confidential issues on disaster recovery strategy.

5.4.2 Questionnaire Development

The questionnaires for the survey were designed to meet the purpose of the research and also to answer the research questions. The table below shows how the researcher designed the survey questionnaires.

Table 5.2

Hypothesis	**Factors**	**No. of questions**
Perceived behavioral control (PBC) will have an effect on the intention to develop an ISDR planning in the Ghanaian banking sector.	Perceived behavioral control (PBC)	3
Subjective norms (SN) will have an effect on the intention to develop an ISDR planning in the Ghanaian banking sector.	Subjective norms (SN)	5
Attitude toward ISDRP compliance will have an effect on intention ISDR planning in the Ghanaian banking sector.	Attitude toward ISDRP	4
Self-efficacy (SE) will have an effect on the intention to develop ISDR planning in the Ghanaian banking sector.	Self-efficacy (SE)	3
Response cost (RC) will have an effect on the intention to develop an ISDR planning in the Ghanaian banking sector.	Response cost (RC)	4
Response efficacy (RE) will have an effect on the intention to develop an ISDR planning in the Ghanaian banking sector	Response efficacy (RE)	4
Perceived severities (PS) will have a positive effect on the intention to develop an ISDR planning in the Ghanaian banking sector.	Perceived severities (PS)	5
Perceived vulnerability (PV) will have a positive effect on the intention to develop an ISDR planning in the Ghanaian banking sector.	Perceived vulnerability (PV)	4
	Motivation or intention to develop an ISDRP	4

The table above shows the factors that the researcher used in the study and the hypothesis that were formed for each of the factors as well as the number of questions asked under each

factor. This was done to enable the researcher under take a survey which in the realism paradigm is very crucial as it helps the realist to triangulate with other data collected. The researcher administered the questionnaires among the manager from the seven financial institutions that agreed to continue with the study.

5.4.3 Data Collection

Data was collected among the seven banking institutions in Ghana on a purposive basis. The questionnaires were left with the organisations to complete after which they called me to fetch them. In all 207 completed questionnaires were returned.

5.5 Mode of Analysis

5.5.1 Quantitative Analysis

The survey questionnaires were coded and entered into the SPSS software (version 20.0) in order to run the analysis. The data set was screened and cleaned. This was done to rectify mistakes that occurred during data entering. A frequency table was generated to have a fair knowledge on the characteristics of the respondents such as gender, age, education and so on. An exploratory analysis which involved the assessment of normality, presentation of descriptive statistics and examination of internal consistency measures for each of the key construct was run. Before testing each of the hypotheses formulated the data for each variable was screened for both skewness and kurtosis. Following this a correlation analysis was also run to check the relationship between the independent variables against the criterion variable (ie motivation and intention to develop an ISDRP). This was followed by the examination of the hypothesis formulated for the study.

5.6 Summary

The aim of this chapter was to present the methodology used in this study. It can be summarized as follows: the researcher discussed a methodological review and posit that the current study is exploratory and the method used was both qualitative and quantitative, the data collection method is primary in nature, the data analysis technique used is multivariate and thematic analysis. Careful attention has been given to create high reliability validity in the study.

CHAPTER SIX

RESEARCH ANALYSIS AND DISCUSSION

6.1 Introduction

This chapter presents the results of the study and is organized into three main sections: background of the sample, examination of the hypotheses, and brief summary of the chapter. To examine the hypotheses, correlational and hierarchical regression analyses were used to test the hypothesized model of motivation and intension to develop ISDRP and identify important relations between the variables of interest. Prediction methods, such as hierarchical regression, are helpful in determining which set of variables, or predictors, are most closely linked to a specific outcome (Green, 1991).

6.2 Background of the study

Two hundred and seven (207) managers participated in this study. The participant's backgrounds, i.e., gender, age, level of completed education and the number of years worked in the organisation are examined in the following sections.

Table 6.1: ***Frequency Table of Demographic Variables***

Category	Variables	*f*	Percent
Gender	Male	117	56.5
	Female	90	43.5
	Total	207	
Age	18-24	21	10.1
	25-30	94	45.4
	31-35	56	27.1
	36-40	30	14.5
	>40	6	2.9
	Total	207	
Education	Bachelor's Degree	146	70.6
	Master's Degree	53	25.6
	PHD (Doctorate)	4	1.9
	Professional	4	1.9
	Total	207	
Years with organisation	1-5	54	26.1
	6-10	67	32.3
	11-15	34	16.4
	Over 15	19	9.7
	Total	174	
	Missing	33	15.8

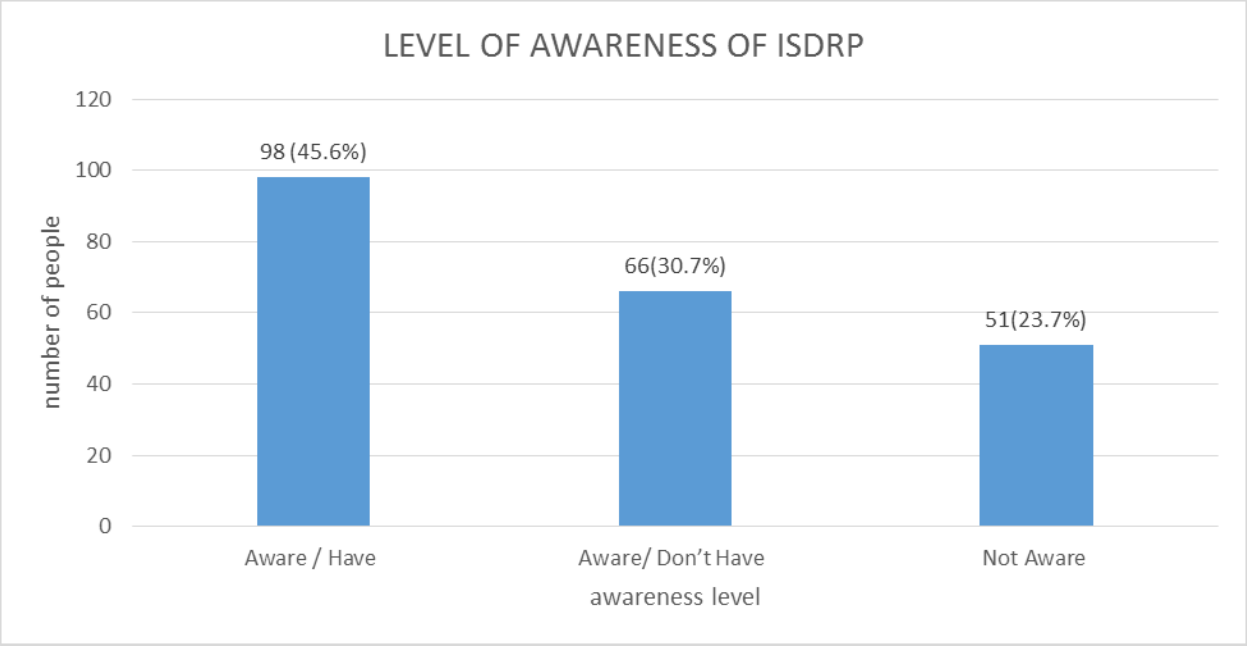
From Table 6.1 above, approximately 43.5% (n = 90) of the sample was female and 56.5% (n = 117) of the sample was male. A frequency analysis of age indicated that 10.1% (*n* = 21) of the respondents reported belonging to the 18-24 group, 45.4% (*n* = 94) to the 25-30 group, 27.1% (*n* = 56) to the 31-35 group, 14.5% (*n* = 30) to the 36-40 group, 2.9% (*n* = 6) belonged to the group greater than 40.

A frequency analysis of highest education completed indicated 70.6% (*n* = 146) of the participant's highest educational attainment was a bachelor's Degree, 25.6% (*n* = 53) reported earning a master's Degree, 1.9% (*n* = 4) reported earning a PHD, while 1.9% (*n* = 4) reported earning other professional degree.

A frequency analysis of year of work with organisation completed indicated 26.1% (n = 54) of the participant's had worked for a period of 1-5 years with their organisation, 32.3% (n = 67) reported having worked for 6-10 years in their organisation, 16.4% (n = 34) reported having worked for 11-15 years in their organisation, whereby, 9.7% (n= 19) reported they have worked for over 15 years in their organisation. Approximately 15.8% (n= 33) of the respondents did not report their years of work with their organisation.

6.3 Extent of awareness of ISDRP among organisation in the Ghanaian banking sector.

Fig 6.1 Extent of awareness of ISDRP among organisation in the Ghanaian banking sector



N=207

Data gathered from the survey showed that 45.6% of the sample size (n= 98) were aware and had an ISDRP in their organisation. On the other hand, 30.7% of the sample size (n= 66) were also aware of ISDRP but they don't have it in their organisation. However, 23.7% of the sample size (n= 51) were not aware of ISDRP at all.

6.4 Exploratory Analysis

The exploratory analysis involved the assessment of normality, presentation of descriptive statistics and examination of internal consistency measures for each of the key construct. Before testing each of the hypotheses formulated the data for each variable was screened for both skewness and kurtosis as shown in Table 6.2

Table 6.2 Exploratory Analysis

Variable	Minimum	Maximum	Mean	SD	Skewness	Kurtosis	Alpha
PV	1.00	5.00	3.76	.87	-1.03	1.14	.62
PS	1.00	5.00	3.836	.73	-1.13	2.50	.63
RS	1.50	5.00	3.29	.87	.12	-.68	.70
RE	1.00	5.00	3.55	.72	-.81	2.07	.64
SE	1.00	5.00	3.54	.92	-.71	.29	.82
ATISDRP	1.00	5.00	4.06	.81	-1.54	3.37	.80
SN	1.00	5.00	3.25	.94	-.35	-.37	.86
PBC	1.00	5.00	3.55	.87	-.50	-.23	.72
MIDISDRP	1.00	5.00	4.00	.66	-1.78	5.89	.68

PV is Perceived Vulnerability scale. PS is Perceived Severity scale. RC is Response Cost scale. RE is Response Efficacy scale. SE is Self- Efficacy. ATISDRP is Attitude towards Information Systems Disaster Recovery Planning. SN is Subjective Norms. PBC is Perceived Behavioral Control. MIDISDRP is Motivation and Intention to develop an Information Systems Disaster Recovery Planning. *N= 207*.

In assessing the normal distribution of the data, skewness and kurtosis indexes were used for each of the key construct. Following Kline's (2005) rules of thumb, absolute values of skew index less than 3 and kurtosis index below 10 suggest that the data is normally distributed. The skewnes and kurtosis indexes as shown in Table 6.2 reveal that all the variables are normally distributed. Hence, the assumption of normality was met for the use of parametric statistics (ie Correlational and regression analysis) for the hypothesis testing. Furthermore the

reliability estimates for the measures were computed to establish the internal consistency of each construct. All the constructs had satisfactory reliabilities which ranged from .62 to .86 as suggested by Nunnally and Bernstein (1994). The reliability estimates were assessed using the cronbach alpha.

6.5 Examination of Hypotheses

Multicollinearity occurs when variables are so highly correlated that it is difficult to obtain reliable estimates of their individual regression coefficients (Cohen & Cohen, 1983). When two variables are highly correlated, they are basically measuring the same phenomenon. To avoid multicollinearity, correlation coefficients between predictor variables greater than .90 should be removed or combined (Green, 1991). High intercorrelations of predictors increase the standard error of the beta coefficients and make assessment of the unique role of each predictor variable difficult (Green & Salkind, 2005; Tabachnick & Fidell, 2001). Intercorrelations were checked and no correlation between predictor variables was found to be greater than .90. As a result no coefficients were removed. Furthermore, the variance inflated factor (VIF) and tolerance scores were assessed. The VIF for each variable was below 5 and the corresponding tolerance value was above .2 (Field 2007; Greene, 2000). Hence there were no endogenuity among the independent variables. Hence, the data was exogeneous.

6.6 Correlation Analysis

In addition to the assumptions of normality and multicollinearity, the correlation among each of the study variables was computed. The summary of the bivariate correlation coefficients among the variables used for the study is reported in Table 6.3

Table 6.3 Correlation, VIF and tolerance indices among the study variable

Variables	PV	PS	RC	RE	OE	ATISDRP	SN	PBC	MIDISDRP
PV	--								
PS	.46***	--							
RC	.08	.22**	--						
RE	.42***	.63***	.38***	--					
SE	.34***	.52***	.25***	.59***	--				
ATISDRP	.52***	.62***	.05	.49***	.45***	--			
SN	.14	.20**	.34***	.33***	.29***	.08	--		
PBC	.42***	.48***	.28***	.55***	.27***	.37***	.49***	--	
MIDISDRP	.37***	.53***	.31***	.43***	.43***	.51***	.18**	.46***	--
VIF	1.529	2.242	1.279	2.431	1.776	1.952	1.487	1.971	
Tolerance	.654	.446	.782	.411	.563	.512	.673	.507	

Note. ** $p < .01$, *** $p < .001$. PV is Perceived Vulnerability scale. PS is Perceived Severity scale. RC is Response Cost scale. RE is Response Efficacy scale. SE is Self-Efficacy. ATISDRP is Attitude towards Information Systems Disaster Recovery Planning. SN is Subjective Norms. PBC is Perceived Behavioral Control. MIDISDRP is Motivation and Intention to develop an Information Systems Disaster Recovery Planning. *N= 207.*

The bivariate correlation as indicated in Table 6.3 revealed that motivation and intention to develop an ISDRP was positively and significantly correlated with perceived vulnerability ($r = .37$, $p < .001$) and perceived severity ($r = .53$, $p < .001$) which is conceptualized as threat appraisal in the integrated model of PMT and TPB used in this study. Accordingly, threat appraisal correlated with motivation and intention to develop an ISDRP. Furthermore, the criterion variable thus motivation and intention to develop an ISDRP was positively and significantly correlated with response cost ($r = .31$, $p < .001$), response efficacy ($r = .43$, $p < .001$) and self-efficacy ($r = .43$, $p < .001$) which is conceptualized as coping appraisal in the model used for the study. Hence, it is evident that all the variables in the PMT applied to this

study are positively and significantly correlated with motivation and intention to develop an ISDRP.

Additionally, motivation and intention to develop an ISDRP was positively and significantly correlated with attitude towards developing an ISDRP (r = .51, p < .001), subjective norms (r = .18, p < .01) and perceive behavioral control (r = .46, p < .001) which are the variables for the theory of planned behavior (TPB) used in this study.

6.6.1 Analyses of Hypotheses 1-3

Hierarchical multiple regression analyses were performed to test H_1-H_3 which stated that after controlling for the demographic variables (gender, age, education and tenure), attitude towards developing ISDRP, subjective norms (SN)and perceive behavioral control (PBC) would predict unique variance in motivation and intention to develop an ISDRP. The results of the hierarchical regression analysis for H1-H3 are presented in Table 6.4

Table 6.4 Summary of hierarchical regression analysis for attitude, subjective norms, perceived behavioral control, and motivation and intention to develop an ISDRP.

Variable	*β*	R^2	ΔR^2	*F-statistic*
Step 1				
Gender	.11	.04	.04	2.30
Age	.12			
Education	-.18*			
Tenure	.04			
Step 2				
ATISDRP	.52***	.29	.25***	16.69***
Step 3				
ATISDRP	.50***	.31	.02*	15.19***
Subjective norms	.14*			
Step 4				
ATISDRP	.39***	.38	.07***	17.40***
Subjective norms	-.01			
PBC	.33***			

Note. $N = 207$, * $p < .05$, *** $p < .001$. ATISDRP is Attitude towards Information Systems Disaster Recovery Planning. SN is Subjective Norms. PBC is Perceived Behavioral Control.

A four step hierarchical multiple regression analysis was conducted with motivation and intention to develop an ISDRP as the criterion variable. Hierarchical multiple regression was used to examine the relationship between a set of independent variables and a dependent variable, after controlling for the effects of some other independent variable on the dependent variable. The demographic variables of gender, age, education and tenure were entered at step one of the regression model to control for their effects on the criterion variable. Subsequently, attitude towards developing ISDRP and subjective norms were entered at steps 2 and 3 of the regression model respectively. Finally, PBC was entered in the last step of the regression model. The hierarchical multiple regression statistics are presented in Table 6.4

The hierarchical multiple regression analysis revealed that after controlling for gender, age, education and tenure, attitude ($\beta = .52$, $\Delta R^2 = .25$, $p < .001$) contributed significantly to the motivation and intention to develop an ISDRP, F (5, 201) = 16.69, $p < .001$. Attitude towards developing ISDRP accounted for 29% of the variance in motivation and intention to develop ISDRP. Again, the addition of subjective norm ($\beta = .14$, $\Delta R^2 = .02$, $p < .05$) contributed significantly to the regression model [F (6, 200) = 15.19, $p < .05$] and explained 31% of the variation in the criterion variable.

Finally, the inclusion of perceive behavioral control ($\beta = .33$, $\Delta R^2 = .07$, $p < .001$) to the regression model [F (7, 199) = 17.40, $p < .001$] explained 38% of the variance in motivation and intention to develop ISDRP. Thus, the most significant antecedent of motivation and intention to develop ISDRP was attitude towards developing an ISDRP which uniquely accounted for 29% of the variance in motivation and intention to develop ISDRP. From the

foregoing discussion, it could be stated that H_1, H_2 and H_3 are validated by the hierarchical multiple regression analysis.

6.6.2 Analyses of Hypotheses 4 - 8

Hierarchical multiple regression analyses were performed to test H_4 –H_8, which stated that after controlling for the demographic variables (gender, age, education and tenure), self-efficacy, response cost, response efficacy, perceived severity and perceived vulnerability would predict unique variance in motivation and intention to develop an ISDRP. The results of the hierarchical regression analysis for H_4-H_8 are presented in Table 6.5

Table 6.5 Summary of hierarchical regression analysis for self-efficacy, response cost, response efficacy, and intention to develop an ISDRP.

Variable	*β*	R^2	ΔR^2	*F- statistic*
Step 1				
Gender	.32	.04	.04	2.3
Age	.06			
Education	-.07*			
Tenure	-.01			
Step 2				
Perceive vulnerability	.16*	.32***	.27***	15.4***
Perceive severity	.45***			
Step 3				
Perceive vulnerability	.13*	.37**	.05**	12.6***
Perceive severity	.34***			
Self-efficacy	.16*			
Response cost	-.01**			
Response efficacy	.18			

*Note. N = 207, * p < .05, ** p < .01, *** p < .001*

A three step hierarchical multiple regression analysis was also conducted with motivation and intention to develop an ISDRP as the criterion variable. The demographic variables of gender, age, education and tenure were entered at step one of the regression model to control for their effects on the criterion variable. Subsequently, perceive vulnerability and perceive

severity which is conceptualized as threat appraisal in Rogers (1983) PMT model, was entered at steps 2. Also, coping appraisal (i.e., self-efficacy, response cost and response efficacy) was entered at step 3 of the regression model. The hierarchical multiple regression statistics are presented in Table 6.5.

The hierarchical multiple regression analysis revealed that after controlling for gender, age, education and tenure, the components of threat appraisal, perceive vulnerability (β = .16, p < .05) and perceive severity (β = .45, p < .001) contributed significantly to the motivation and intention to develop an ISDRP model, F (6, 200) = 15.37, p < .001. Further, threat appraisal recorded an R^2 change of .27 and accounted for 32% of the variance in motivation and intention to develop ISDRP. Again, the addition of response cost (β = -.01, p < .01), response efficacy (β = .18, p > .05) and self-efficacy (β = .16, p < .05) in step 3 of the regression model contributed significantly to the regression model [F (9, 197) = 12.65, p < .05] and explained 37% of the variation in the criterion variable. Hence, the most significant antecedent of motivation and intention to develop ISDRP under threat appraisal was perceived severity. Regarding coping appraisal, response efficacy was the most significant predictor of motivation and intention to develop ISDRP. Response cost had a negative beta coefficient of -.01 which reveals that response cost will have a negative effect on motivation and intention to develop an ISDRP. It can therefore be concluded that apart from H_5 which was not supported, H_4, H_6, H_7 and H_8 were validated by the hierarchical multiple regression analysis.

Table 6.7 Summary of results

Number	Hypothesized path	β	Result
H_1	Perceived behavioral control → motivation and intention	.33	Supported
H_2	Subjective norms → motivation and intention	.14	Supported
H_3	Attitude → motivation and intention	.52	Supported
H_4	Self-efficacy → motivation and intention	.16	Supported
H_5	Response cost → motivation and intention	-.01	Not supported
H_6	Response efficacy → motivation and intention	.18	Supported
H_7	Perceived severity → motivation and intention	.45	Supported
H_8	Perceived vulnerability → motivation and intention	.16	Supported

6.8 Discussion of results

By integrating two relevant theories that are protection motivation theory and the theory of planned behavior, this study enriched our understanding of the ISDRP in the Ghanaian banking sector. The study's results showed that a significant amount of variance in motivation and intention to develop an ISDRP in the Ghanaian banking sector was explained by the independent variables used in the study. Guided by the integration of the aforementioned theories, the following section discusses the results of each hypothesis tested. The results of this study suggested that there were statistically significant and meaningful relations to explore among the variables of interest. First H_1-H_3 (theory of planned behavior) is explored followed by H_4-H_8 (protection motivation theory).

6.8.1 Hypotheses 1-3 (Theory of Planned Behavior)

The first hypothesis stated that perceived behavioral control (PBC) of managers will have a positive effect on motivation and intention to develop an ISDRP. Results from the correlation analysis indicated there was a positive and significant relation between PBC and motivation and intention to develop an ISDRP in the Ghanaian banking sector. Findings show support for H_1, and thus the null hypothesis was rejected. This supports the findings of other

researchers. Wall, Devine-Wright and Mils (2007), for example, found that PBC and moral norm were the only variables to predict intention secure organisational assets within a bank. Harland, Staats and Wilke (1999) found PBC to be the strongest predictor of intention to use modes of transport other than a car. In their study they examined five environmentally positive behaviors and showed that the importance of PBC varied by behavior. This was also the case in this study. Even though PBC was not the strongest predictor for behavioral intention in this study, it had a positive and significant relation with the criterion variable.

The second hypothesis stated that subjective norms (SN) of managers will have a positive effect on the motivation and intention to develop an ISDRP. The correlation analysis revealed there was a positive and significant relation between SN and motivation and intention to develop an ISDRP in the Ghanaian banking sector. Hence, H_2 was supported and thus the null hypothesis was rejected. This finding corroborates the work of Bamberg and Schmidt (2003), who found a significant influence of social expectations on intention for a bank to secure its information systems. More specifically, it suggests that their findings were specific to a particular bank's population, which they believe could have skewed their finding to one particular direction, is untrue. This study large sample shows that social expectations have a robust effect on intentions and habits, irrespective of age or occupational group.

The third hypothesis stated that attitude towards developing ISDRP will have a positive effect on the criterion variable. Results from the correlation analysis indicated there was a positive and significant relation between attitude and motivation and intention to develop an ISDRP. Findings show support for H_3, and thus null hypothesis was rejected. This finding is in congruence with some previous research by Ifinedo (2012) which revealed that attitude will have a positive effect on ISSP compliance. The results from the aforementioned study is in

accordance with that of this current study which revealed that attitude towards developing an ISDR plan is the strongest predictor for developing ISDRP among the variables in the TPB.

6.8.2 Hypothesis 4-8 (Protection Motivation Theory)

H_4 stated that self- efficacy (SE) of managers will have a positive effect on the motivation and intention to develop an ISDRP. Results from the correlation analysis indicated there was a positive and significant relation between SE and motivation and intention to develop an ISDRP in the Ghanaian banking sector. Findings show support for H_4, and thus the null hypothesis was rejected. Notably, self-efficacy has been recognized as one of the important components for predicting behavioral intention (Lwin & Saw, 2007; Wurtele & Maddux, 1987). Published studies have documented the effect of self -efficacy in predicting smoking behaviour (Gwaltney, Metrik and Shiffman, 2009). In this study, it was found that self-efficacy, was among the predictors of motivation and intention to develop an ISDRP. This suggests the importance of promoting self-efficacy in developing an ISDRP among organisations in the Ghanaian banking sector.

H_5 stated that response cost (RC) of managers will have a positive effect on the motivation and intention to develop an ISDRP. However, results from the correlation analysis indicated there was a negative relation between RC and the criterion variable. The findings show support for the null hypothesis. Hence the null hypothesis was accepted. The direction of the relationship is consistent with prediction and findings elsewhere (Lee & Larsen, 2009; Workman et al., 2008) however, the strength of the relationship is inadequate to affirm the stated hypothesis. Similar studies (e.g. Herath & Rao, 2009a) that examined the effect of response cost on ISSP behavioral compliance presented a view comparable to the one being presented herein i.e. response cost did not significantly influence compliance intentions. Hence, the null hypothesis for response cost was accepted. A plausible reason for this result

may be due to sample composition and research design. For example, it is possible that while some participants may have positive view of the cost/benefit of developing ISDRP in their contexts; others may have differing perspectives on the issue. Workman et al. (2008) had asserted peoples' perception of this factor tend to vary.

The sixth hypothesis stated that response efficacy (RE) of managers will have a positive effect on the motivation and intention to develop an ISDRP. Results from the correlation analysis indicated there was a positive and significant relation between RE and motivation and intention to develop an ISDRP. Findings show support for H_6, and thus the null hypothesis was rejected. Similarly, previous PMT studies have found response efficacy to have a significant association with intention and behavior (Plotnikoff & Higginbotham, 2002; Stanley & Maddux, 1986; Wurtele & Maddux, 1987).

H_7 stated that perceived severity of will have a positive effect on the motivation and intention to develop an ISDRP in the Ghanaian banking sector. Results from the correlation analysis indicated there was a positive and significant relation between PS and motivation and intention to develop an ISDRP. Findings show support for H_7, and thus the null hypothesis was rejected. This is somewhat expected as it is logical to expect that an individual's perception of risks, vulnerability, security breaches and attacks will motivate them to develop an ISDRP for the organisation. However, this finding contradicts Ifinedo (2012) study on ISSP compliance were perceive severity had a negative effect in ISSP compliance. This result might have been impacted by contextual or extraneous influences. On the other hand, a study by Lee (2010) showed that perceive severity significantly affect faculty members' intentions to adopt anti-plagiarism software. That is, the decision of faculty members to adopt software is influenced by the perceived severity of the negative consequences of Internet plagiarism.

This result was in accordance with that of this current study.

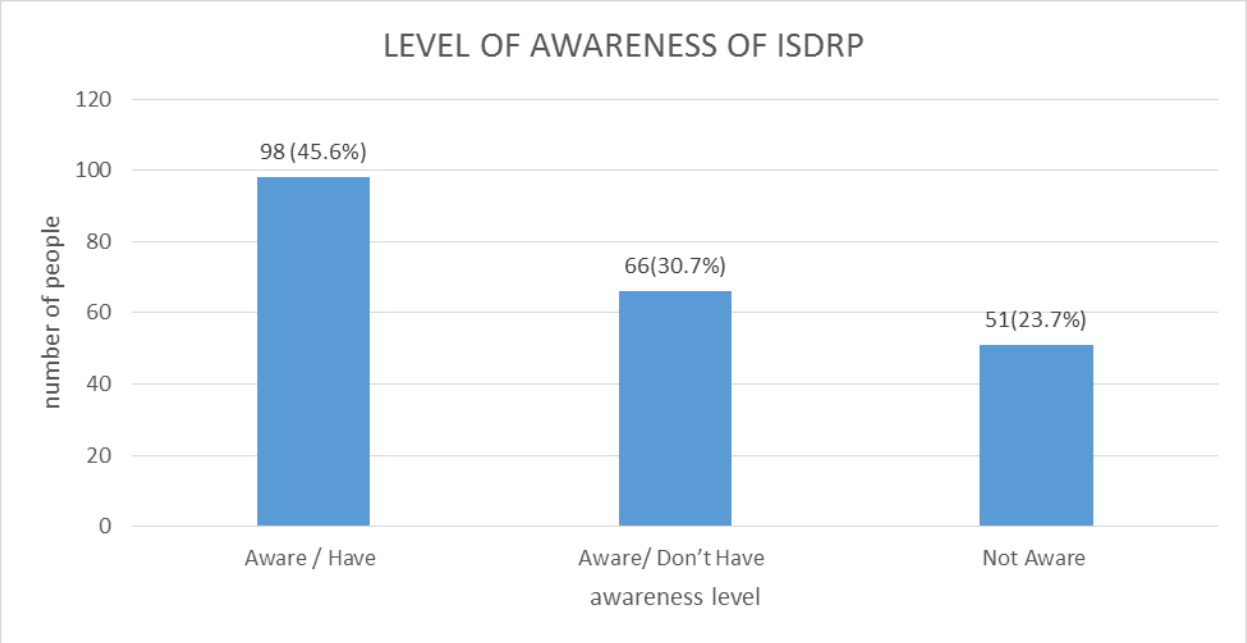
H_8 stated that perceived vulnerability (PV) of managers will have a positive effect on the motivation and intention to develop an ISDRP. Results from the correlation analysis indicated there was a positive and significant relation between PV and motivation and intention to develop an ISDRP. Findings show support for H_7, and thus the null hypothesis was rejected. This finding is generally congruous with previous research that used PMT (Plotnikoff & Higginbotham, 1995; Plotnikoff & Higginbotham, 1998). In contrast to the discussion above, Workman et al. (2008) noted that vulnerability was insignificant in explaining the likelihood of employees conforming to IS security precautions. It appears that the respondents of this study generally believed that they would be subjected to information systems disaster threats if they do not comply with the ISDRP process.

In conclusion, the findings of the quantitative analysis revealed that all the variables of the theory of planned behavior (perceived behavioral control, subjective norms and attitude) had a positive and significant effect on the criterion variable thus intention and motivation to develop an ISDRP. Hence it could be concluded that PBC, SN and attitude are predictors for motivation and intention to develop ISDRP in organisations in the Ghanaian banking sector. On the other hand, PV, PS, SE, RE had a positive and significant effect on the dependent variable with the exception of response cost (RC) with had a significant negative effect on the criterion variable. It can therefore be concluded with the exception of RC all the other variables of PMT are predictors for motivation and intention to develop ISDRP in organisations in the Ghanaian banking sector.

6.7 Revisiting the Research Questions

This session of the study provides the answers that were gathered from the survey to respond to the research questions. The answers were provided based on how the questions were formulated in chapter one.

Question one: What is the extent of awareness of ISDRP among organisations in the Ghanaian banking sector?



N=207

Data gathered from the survey showed that 45.6% of the sample size (n= 98) were aware and had an ISDRP in their organisation. On the other hand, 30.7% of the sample size (n= 66) were also aware of ISDRP but they don't have it in their organisation. However, 23.7% of the sample size (n= 51) were not aware of ISDRP at all. Even though 45.6% of the sample size were aware and had an ISDRP in place, a total of 54.4% of organisation in the Ghanaian banking sector don't have an ISDRP. Perhaps, the reason why most of the organisations in the Ghanaian banking sector don't have an ISDRP could be that, they have not come to the

full realization that most of their critical business functions and processes are dependent on information systems. For this reason most of their business operations will come to a halt if disaster should strike their information systems. Another possible reason for this could also be that most organisation in the Ghanaian banking sector have not had any negative experience with disaster so it is assumed that everything okay. These finding are congruent with Wakolbinger & Toyasaki (2011) who indicated that till organisations become fully aware of the essence of information systems to their business, their attitude towards developing a disaster recovery plan for their information systems will be minimal. Hopkins (2010) also revealed that because organisations might not have experienced any disaster, they might think that everything is in shape and that the organisation should not worry of a disaster. This way of thinking sometimes prevents organisations from developing an ISDRP. The aforementioned reasons might have caused the organisation in the Ghanaian banking sector not to adopt an information systems disaster recovery plan. Hence the level of awareness of ISDRP among organisations in the Ghanaian banking sector is to an extent appreciable.

Question two: What are the enablers and inhibitors of information systems disaster recovery planning among organisations in the Ghanaian banking sector?

Data collected from the survey revealed the enablers and inhibitors of ISDRP among organisations in the Ghanaian banking sector. This session highlights on the enablers and inhibitors of ISDRP among the organisations in the Ghanaian banking sector.

The first hypothesis stated that perceive behavioral control (PBC) will have a positive effect on motivation and intention to develop an ISDRP among organisations in the Ghanaian banking sector. Results from the correlation analysis indicated there was a positive and

significant relation between PBC and motivation and intention to develop an ISDRP. This supports the findings of other researchers. Wall, Devine-Wright and Mils (2007), for example, found that PBC and moral norm were the only variables to predict intention to drive. Harland, Staats and Wilke (1999) found PBC to be the strongest predictor of intention to use modes of transport other than a car. In their study they examined five environmentally positive behaviors and showed that the importance of PBC varied by behavior. This was also the case in this study. Even though PBC was not the strongest predictor for behavioral intention in this study, it had a positive and significant relation with the criterion variable i.e. motivation and intention to develop an ISDRP. Hence perceive behavioral control according to the analysis of this study is an enabler of ISDRP among organisations in the Ghanaian banking sector.

The second hypothesis stated that subjective norms (SN) will have a positive effect on the motivation and intention to develop an ISDRP among organisation in the Ghanaian banking sector. The correlation analysis revealed there was a positive and significant relation between SN and motivation and intention to develop an ISDRP. This finding corroborates the work of Bamberg and Schmidt (2003), who found a significant influence of social expectations on intention to use a car. More specifically, it suggests that their findings were specific to a student population, who are young and sensitive to social expectations, is untrue. This studies large sample shows that social expectations have a robust effect on intentions and habits, irrespective of age or occupational group. Hence subjective norms according to the analysis of this research are an enabler of information systems disaster recovery planning among organisations in the Ghanaian banking sector.

The third hypothesis stated that attitude towards developing ISDRP will have a positive effect on the criterion variable. Results from the correlation analysis indicated there was a positive

and significant relation between attitude and motivation and intention to develop an ISDRP among organisation in the Ghanaian banking sector. The results from the aforementioned studies are in support with that of this current study which revealed that attitude towards developing an ISDRP is the strongest predictor for developing ISDRP among organisations in the Ghanaian banking sector. Hence attitude like the aforementioned factors is also an enabler of ISDRP among organisations in the Ghanaian banking sector.

The fourth hypothesis for this study stated that self- efficacy (SE) will have a positive effect on the motivation and intention to develop an ISDRP among organisations in the Ghanaian banking sector. Results from the correlation analysis indicated there was a positive and significant relation between SE and motivation and intention to develop an ISDRP. Notably, self-efficacy has been recognized as one of the important components for predicting behavioral intention (Lwin & Saw, 2007; Wurtele & Maddux, 1987). Published studies have documented the effect of self -efficacy in predicting smoking behavior (Gwaltney, Metrik & Shiffman, 2009). In this study, it was found that self-efficacy, was among the predictors of motivation and intention to develop an ISDRP in banking organisations in Ghana. This suggests the importance of promoting self-efficacy in developing an ISDRP among organisations in the Ghanaian banking sector. Self-efficacy is therefore an enabler of ISDRP among organisations in the Ghanaian banking industry.

The sixth hypothesis stated that response efficacy (RE) will have a positive effect on the motivation and intention to develop an ISDRP among organisation in the Ghanaian banking sector. Results from the correlation analysis indicated there was a positive and significant relation between RE and motivation and intention to develop an ISDRP. Similarly, previous PMT studies have found response efficacy to have a significant association with intention and behavior (Plotnikoff & Higginbotham, 2002; Stanley & Maddux, 1986; Wurtele & Maddux,

1987). Hence it can be concluded that response efficacy is an enabler of ISDRP among organisation in the Ghanaian banking sector.

Perceived severity will have a positive effect on the motivation and intention to develop an ISDRP among organisation in the Ghanaian banking sector was the seventh hypothesis formulated. Results from the correlation analysis indicated there was a positive and significant relation between PS and motivation and intention to develop an ISDRP. This is somewhat expected as it is logical to expect that an individual's perception of risks, vulnerability, security breaches and attacks will motivate them to develop an ISDRP for the organisation. However, this finding contradicts Ifinedo (2012) study on ISSP compliance were perceive severity had a negative effect in ISSP compliance. This result might have been impacted by contextual or extraneous influences. On the other hand, a study by Lee (2010) showed that perceive severity significantly affect faculty members' intentions to adopt anti-plagiarism software. That is, the decision of faculty members to adopt software is influenced by the perceived severity of the negative consequences of Internet plagiarism. This result was in accordance with that of this current study. The analysis for this study proved that perceived severity is an enabler of ISDRP among organisation in the Ghanaian banking sector.

Finally, the eighth hypothesis stated that perceived vulnerability (PV) will have a positive effect on the motivation and intention to develop an ISDRP among organisation in the Ghanaian banking sector. Results from the correlation analysis indicated there was a positive and significant relation between PV and motivation and intention to develop an ISDRP. This finding is generally congruous with previous research that used PMT (Plotnikoff & Higginbotham, 1995; Plotnikoff & Higginbotham, 1998). In contrast to the discussion above, Workman et al. (2008) noted that vulnerability was insignificant in explaining the likelihood of employees conforming to IS security precautions. It appears that the respondents of this

study generally believed that they would be subjected to information systems disaster threats if they do not comply with the ISDRP process. There is can be concluded that perceived vulnerability is an enabler of ISDRP among organisation in the Ghanaian banking sector.

The fifth hypothesis stated that response cost (RC) will have a positive effect on the motivation and intention to develop an ISDRP. However, results from the correlation analysis indicated there was a negative relation between RC and the criterion variable. The findings show support for the null hypothesis. The direction of the relationship is consistent with prediction and findings elsewhere (Lee & Larsen, 2009; Workman et al., 2008) however, the strength of the relationship is inadequate to affirm the stated hypothesis. Similar studies (e.g. Herath & Rao, 2009a) that examined the effect of response cost on ISSP behavioral compliance presented a view comparable to the one being presented herein i.e. response cost did not significantly influence compliance intentions. Hence, the null hypothesis for response cost was accepted. A plausible reason for this result may be due to sample composition and research design. For example, it is possible that while some participants may have positive view of the cost/benefit of developing ISDRP in their contexts; others may have differing perspectives on the issue. Workman et al. (2008) had asserted peoples' perception of this factor tend to vary. Hence, response cost proved not to be an enabler of ISDRP among organisations in the Ghanaian banking sector.

The data gathered revealed that lack of management awareness of ISDRP among banking organisations in Ghana is an inhibitor of an ISDRP. Management is assumed to have the strategic eye for the organisation; they know where they want to take the organisation to, so if they are not aware of the effect of disaster on their IS, having an ISDRP will not be in their priority list for the organisation. This finding from the study supports other findings in various IS literature. Brynjolfsson & Schrage (2009) disclosed that lack of management

awareness to the ISDRP can constrain the planning process of developing an ISDRP. As indicated by Gordon and Tarafdar (2010) it is senior management that is ultimately accountable and charged with the task of initiating and supporting important projects with adequate funding and resources. So if managers are not made aware of ISDRP it is likely the plan would not materialize but even if it does it will not receive the necessary support it deserves. Lack of management awareness in ISDRP is therefore an inhibitor of ISDRP among organisations in the Ghanaian banking sector.

The findings further revealed that lack of security awareness and training for all staff could be an inhibitor to a successful ISDRP among banking organisations in Ghana. If employees or staff are not well trained on security especially with regards to there IS, planning for ISDRP will be difficult. This finding corroborates with previous research on ISDRP. Hopkins (2010) is of the opinion that lack of security awareness and training for all staff could be an inhibitor to a successful ISDRP. Training of staff on ISDRP is a very critical issue in organisations since the plan against disaster has to be designed and implemented by the staff of the organisation. Inadequate training (Han & Mithas, 2011) of staff will lead to loop holes in the disaster recovery plan. Lack of security awareness can also hinder ISDRP in that the employees or managers will not see the reason why they should provide security for their information assets. All these without any doubt can be said to hinder a successful disaster recovery planning. And this can affect the operations of organisations.

Additionally, findings from this research revealed that lack of allocated funds due to low priority for ISDRP among organisations in the Ghanaian banking sector is an inhibitor to a successful information systems disaster recovery plan. This finding supports findings in other studies elsewhere. For example, King (2008) identified lack of allocated funds as an inhibitor

of a successful ISDRP. . If planning against disaster is not on the priority list of organisations, it is of no doubt that much funds will not be allocated for it. And without sufficient and necessary funds a proper and effective DRP cannot be developed but even if it is developed it cannot secure or protect the necessary information it must if disaster strikes (Carr 2008).

6.8 Summary

With respect to the purpose of this research, this study used the theory of planned behavior and the protection motivation theory to investigate the drivers and inhibitors of information systems disaster recovery planning among organisations in the Ghanaian banking sector. Further, the measures these organisations put in place to address the inhibitors were also investigated. The study revealed that entities have powers and liabilities which can influence the process of developing an ISDRP.

CHAPTER SEVEN

CONCLUSION AND RECOMMENDATION

7.1 Summary

This study began with the purpose of investigating the enablers and inhibitors of information systems disaster recovery planning in organisations in the Ghanaian banking sector. The research adopted a quantitative method approach to analyze the phenomenon under study. Survey questionnaires were used as the main data collection tool for the quantitative analysis. The survey was conducted in seven different banking institutions in Ghana. A total of 207 respondents were sampled for the survey. Data collected was analyzed using some descriptive statistics and a regression analysis.

In the literature review, the framework used for the study was mentioned with detailed discussion of it in chapter three of the study. The framework hypothesized that perceived vulnerability (PV), perceived severity (PS), response cost (RC), response efficacy (RE) and self- efficacy (SE) will have a positive effect on motivation and intention to develop an ISDRP. Whereas, perceive behavioral control (PBC), subjective norms (SN), and attitude will also have a positive effect on the criterion variable.

However, the analysis and discussion of the study revealed that with the exception of response cost (RC) which had a negative effect on the criterion variable, all the remaining factors predicted positively to the dependent variable. Revealing that PV, PS, RE, SE, PBC, SN, and attitude are predictors of motivation and intention to develop an ISDRP within organisations in the Ghanaian banking sector.

7.2 Implication to Research, Policy and Practice

Concerning research implication, the study adds to some of the already existing literature on disaster recovery planning within the IS discipline. This research proposes and validates a research conceptualization that integrates PMT and TPB in the context of managers ISDR planning intention. To that end, this research indicates that the fusion of both theoretical frameworks permits a better understanding of the sorts of factors that affect managers ISDR planning intention as opposed when each is used alone to investigate the theme (Ifinedo, 2011; Vance, Siponen & Pahnila, 2012).. Hence, the findings from this study contribute significantly to knowledge.

Concerning implication to policy, the results of this study provided the factors that predict motivation and intention to develop ISDRP. Management of organisations can therefore capitalize on these factors by way of educating their employees through seminars and other training programmes pertaining to these factors so as to create the need for an IS DRP.

Concerning implication to practice, the study provided a thorough explanation and discussion on the factors which influence the motivation and intention for the development of information systems disaster recovery planning in Ghana and how to address some of the inhibitors of ISDRP. These factors if properly adhered to can practically motivate organisations to develop an ISDRP.

7.3 Contribution and Future Research Directions

This study has contributed significantly to the information systems discipline. First, it set to investigate ISDRP among organisation in the Ghanaian banking sector. Literature reviewed showed that Africa lacked research on ISDRP (Kgakats & Rautenbach, 2013; Raju &

Niekerk, 2013). Therefore investigating information systems disaster recovery planning in organisation in the Ghanaian banking sector bridges the context gap that exists.

Second, this study is among the few other studies that have integrated the protection motivation theory (PMT) and the theory of planned behavior (TPB) to investigate a phenomenon in the IS domain (Ifinedo, 2012). Results from the findings show that which the exception of Response cost which is a factor of PMT, all other factors were predictors of motivation and intention to develop an ISDRP among organisation in the Ghanaian banking sector. These contributions are very imperative.

This study discussed information systems disaster recovery planning (ISDRP) among work by looking ISDRP from other financial institutions, for example among insurance companies and so on.

This work is not in any way exhaustive. The findings and lessons are stepping stones towards the motivation and intention to develop ISDRP which is rapidly becoming a necessity in organisations. The reality in practice may require more effort and further research. ISDRP can also be studied from the perspective of public sector institution to understand the readiness for regulatory institutions to support the implementation of ISDR plan.

References

Aggelinos, G., & Katsikas, S. (2007). Enterprise Recovery in Health Care. In proceedings of the 12th International Symposium on Health Information Management Research – ISHIMR

Ahmed, A., & Sugianto, L. (2008). "RFID in Emergency Management" in: *RFID & Smart Technologies for Information Convergence,* Information Science Reference, Hershey, USA, p. 350.

Anderson, J. (2008). New trends in backup: Is your disaster recovery plan keeping up?. *The e-Security Advisor, 8* (2), 58.

Aral, S., & Weill, P. (2007). IT Assets, Organisational Capabilities, and Firm Performance: How Resource Allocations and Organisational Differences Explain Performance Variation. *Organisation Science, 18*(5), 763-780.

Attarha, M., & Modiri, N. (2011). "Focusing on the Importance and the Role of Requirement Engineering.*4th International Conference on Interaction Sciences (ICIS)*, 181-184.

Aziagba, P., & Edet, G. (2008). Disaster control planning for academic libraries in West Africa. *The Journal of Academic Librarianship, 34* (3), 265-8.

Baird, A., Jamieson, R., & Cerpa, N., (2002). Development of a Framework for Risks and Security in B2C E-Business, in Monteiro J L, Swatman P M C, Tavares L V, (eds), Towards the Knowledge Society: eCommerce, eBusiness and eGovernment, Kluwer Academic Publishers, 399-414.

Bamberg, S., & Schmidt, P. (2003). Incentives, morality, or habit? Predicting students' car use for university routes with the models of Ajzen, Schwartz, and Triandis. *Environment and Behavior*, *35*, 264–285.

Barbara, L., P. (2008). Identifying and Tracking Disaster Victims: State-of-the-Art Technology Review. *The Journal of Health Promotion and Maintenance, 31* (1), 23-34.

Bardhan, I., R. (2007). Toward a Theory to Study the Use of Collaborative Product Commerce for Product Development. *Information Technology and Management, 8* (2), 167-184.

Basu, V., & Lederer, A. (2011). Agency Theory and Consultant Management in Enterprise Resource Planning Systems Implementation. *ACM SIGMIS Database*, *42* (3), 10-33.

Bennett, E. (2009). Dell CIO on Culture and Web 2.0," available at http://www.cioinsight.com/c/a/Trends/Culture-Czar-443269/ (accessed February 25, 2014.

Berente, N., Baxter, R., & Lyytinen, K. (2010). A dynamic view of innovation and AEC project governance: Knowledge creation across object worlds. *Construction Management and Economics*, *28*(6), 569-588.

Bharosa, N., Lee, J., & Janssen, M. (2010). Challenges and Obstacles in Sharing and Coordinating Information during Multi-agency Disaster Response: Propositions from Field Exercises. *Information Systems Frontiers*, *12* (1), 49–65.

Bisman, J. E. (2002). *The critical realist paradigm as an approach to research in accounting*. Poster presentation at the Accounting Association of Australian and New Zealand Annual Conference, Perth, Australia.

Bjornson, F.O., & Dingsoyr, T. (2008). Knowledge Management in Software Engineering: A Systematic Review of Studied Concepts, Findings and Research Methods Used," *Information and Software Technology 50* (11), 1055-1068.

Boadi, R. A., & Shaik, A. G. (2006). M-commerce Breakthrough in Developing Countries: The role of m-commerce in wealth creation and economic growth in Developing Countries.

Boin, A., & McConnell, A. (2007). Preparing for critical infrastructure breakdowns: The limits of crisis management and the need for resilience. *Journal of Contingencies and Crisis Management*, *15*(1), 50-59.

Boin, A., Kelle, P., & Whybark, D. (2010). Resilient Supply Chains for Extreme Situations: Outlining a New Field of Study. *International Journal of Production Economics*, *126* (1), 1–6.

Boland, R. J., Lyytinen, K., & Yoo, Y. (2007). Wakes of innovation in project networks: The case of digital 3-D representations in architecture, engineering, and construction. *Organisation Science*, *18*(4), 631-647.

Bonner, N. A., Teng, J. T. C. & Nerur, S. (2010). The Perceived Advantage of Agile Development Methodologies by Software Professionals: Testing an Innovation-Theoretic Model, *AMCIS 2010 Proceedings*, Paper 93.

Boyd, M. D., & Ellison, B.N. (2008). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication 13* (1), 210-230.

Briers, M., & Chua, W. F. (2001). The role of actor-networks and boundary objects in management accounting change: a field study of an implementation of activity- based costing. *Accounting, Organisations and Society 26*(3), 237–269.

Brynjolfsson, E., & Schrage, M. (2009). The New, Faster Face of Innovation," *MIT Sloan Management Review Online*, August 17 (http://sloanreview.mit.edu/business-insight/articles/2009/3/51 39/the-new-faster-face-of-innovation/).

Busquets, J. (2010). Orchestrating Smart Business Network Dynamics for Innovation. *European Journal of Information Systems*, *19* (4), 481–493.

Carr, D. F. (2008). Wyeth's Prescription for Business Process Management Success. *CIO*, May30(http://www.cio.com/article/375067/Wyeth_s_Prescription_for_Business_Process_ Management_Success).

Castillo, J. J. (2009). Convenience sampling. Retrieved Feb 27, 2014 from Experiment Resources: http://www.experiment-resources.com/convenience-sampling.html

Choi, S.G., & Johanson, J. (2012). Knowledge Translation through Expatriates in International Knowledge Transfer. *International Business Review*.

Churchland, M., (1989). Scientific realism and the plasticity of the mind. Cambridge University Press.

Cohen, J., & Cohen, P. (1983). Applied multiple regression/correlation analysis for the behavioral sciences (2nd ed.). Hillsdale, NJ: Erlbaum.

Creswell, J. W. (2009). *Research design: Qualitative, Quantitative and Mixed Methods Approaches*, 3rd London: Sage Publication.

Crowe, A. (2010). The Social Media Manifesto: A Comprehensive Review of the Impact of Social media on Emergency Management. *Journal of Business Continuity & Emergency Planning 5* (1), 409 – 420.

Crowe, M. (2007). Today's disaster recovery: A holistic approach to remediation. *Illinois Banker*. *43*(12), 16-17.

Cumbie, B. (2007). The Essential Components of Disaster Recovery Methods: A Delphi Study among Small Businesses. *AMCIS 2007 Proceedings*, Paper 115.

Curtis, G. (2008). Beyond disaster recovery. *Directorship*, *23*(2), 38-42.

Day, J. M., Junglas, I., & Silva, L. (2009). Information Flow Impediments in Disaster Relief Supply Chains. *Journal of the Association for Information Systems*, *10* (8), 637–660.

Drechsler, W., & Natter, M. (2012). Understanding a Firm's Openness Decisions in Innovation. *Journal of Business Research*, *65*(3), 438-445.

Eshghi, K., & Larson, R. C. (2008). Disasters: Lessons from the Past 105 Years. *Disaster Prevention and Management 17* (1) 62-82.

Fabian, F. H. & Dhillon, G. (2007). Losing Managerial Discretion: The Unexplored Risk of Collaborative Information Sharing. *Journal of Information Science and Technology*, *4* (1), 50–62.

Fajardo, J., & Oppus, C. (2010). A Mobile Disaster Management System Using the Android Technology. *WSEAS Transactions on Communications*, *6* (9), 343–353.

FEMA (2009). *Use of social media tools at FEMA* (http://tinyurl.com/yhsv9xn; accessed February 20,2014)

Field, A. P. (2007). Summarizing Data. In G. C. L. Davey (ed.) Complete Psychlogy (2nd edition). London: Holde & Stoughton.

Gao, Y. (2011). Philanthropic Disaster Relief Giving as a Response to Institutional Pressure from China. *Journal of Business Research*, *64* (12), 1377–1382.

Gefen, D., & Carmel, E. (2008). Is the World Really Flat? A Look at Offshoring at an Online Programming Marketplace. *MIS Quarterly 32* (2), 367-384.

George, C.A. (2010). A Framework for Communication of Software Requirements (in a Medium-Sized Engineering Firm in the Plant Automation Industry)." United States -- Pennsylvania: Robert Morris University.

Gerlach, A. (2005). "The development and use of disaster plans: the Berlin experience" Preparing for the Worst, Planning for the Best: Protecting Our Cultural Heritage from Disaster: *Preconference to the 69th IFLA General Conference and Council Proceedings in Berlin, Germany, 2003*, K.G. Saur, Munchen, 95-102.

Gold, L. (2008). Security still tops tech concerns. *Accounting Today*, *22*(3), 25-28

Goldoni, V., & Oliveira, M. (2010). Knowledge Management Metrics in Software Development Companies in Brazil. *Journal of Knowledge Management 14* (2), 301-313.

Gopal, A., & Gosain, S. (2010). The Role of Organisational Controls and Boundary Spanning in Software Development Outsourcing: Implications for Project Performance. *Information Systems Research 21* (4), 960-982.

Gordon, S. R., & Tarafdar, M. (2010). The IT Audit that Boosts Innovation. *Sloan Management Review*, 39-47.

Green, S. B., & Salkind, N. J. (2005). Using SPSS for Windows and Macintosh: Analysing and Understanding Data, 4th edn. (Upper Saddle River, NJ: Prentice Hall).

Green, S. B. (1991). How many subjects does it take to do a regression analysis? Multivariate Behavioral Research, 26, 499-510.

Greene, H. (2000). Econometric Analysis (Fourth edition). Upper Saddle River, NJ: Prentice-Hall.

Gregor, S., & Jones, D. (2007). The anatomy of a design theory. *Journal of the Association for Information Systems*, *8*(5), 312-335.

Grigonis, R. (2002). Disaster Survival Guide for Business Communications Networks: Strategies for Planning, Response, and Recovery in Data and Telecom System", *CMP Books, Gilroy*, CA, 2002.

Guster, D., McCann, B., Krzenski, K., & Lee, O. (2008). A cost effective, safe, and simple method to provide a disaster recovery plan to small and medium businesses," *Review of Business Research* , *8* (4), 63-71.

Gwaltney, C. J., Metrik, J., Kahler, C. W., & Shiffman, S. (2009). Self-efficacy and pro-environmental intentions: The case of commuting-mode choice. *Environment and Behavior*, *39*, 731- 753

Han, K., & Mithas, S. (2011). Does IT Outsourcing Reduce Non-IT Costs for Firms? Theory and Evidence. Working Paper, McGill University, Montreal, Canada.

Harland, P., Staats, H., & Wilke, H. A. M. (1999). Explaining proenvironmental intention and behavior by personal norms and the theory of planned behavior. *Journal of Applied Social Psychology*, 29, 2505-2528.

Harland, P., Staats, H., & Wilke, H. A. M. (1999). Explaining pro-environmental intentions and behavior by personal norms and the theory of planned behavior. *Journal of Applied Social Psychology*, *29*, 2505-2528.

Harnesk, D. (2004). *A framework for Strategic Alignment of Business and Information Technology in Small and Medium sized Firms*. Licentiate thesis, Lulea University of Technology; Department of Business Administration and Social Science.

Harney, N. (2004). Business continuity and disaster recovery: Backup or shutdown. *eDoc Magazine* ,*3* (3), pp. 42-43.

Herath T., & Rao H. (2009a). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125.

Hiltz, S. R., Van de Walle, B. & Turoff, M. (2010). The domain of emergency management information. *Information Systems for Emergency Management*, *4* (2), 3-20.

Hoffman, D. L., & Novak, P. T. (2012). *Need Satisfaction from Interacting with People versus Content: The Roles of Motivational Orientation and Identification with Social Media Groups*. (http://ssrn.com/abstract=1990005, accessed February 20, 2014)

Hopkins, M. S. (2010). The Four Ways IT Is Revolutionizing Innovation. *Sloan Management Review*, Spring, 51-56.

Housel, T., Sawy, O., & Donovan, P. (2006). Information systems for Crisis management: Lessons from south California Edison. *MIS Quarterly*, *10* (4), 399-400

Howden, M. (2009). How Humanitarian Logistics Information Systems Can Improve Humanitarian Supply Chains: AView from the Field" in Landgren, J. and S. Jul (eds.) *Proceedings of the 6th International ISCRAM Conference*, Gothenburg, Sweden.

Idugboe, D. (2011). Why Businesses Should Use Social Media For Disaster Management. (http://smedio.com/2011/02/24/why-businesses-should-use-social-media-for-disastermanagement/, accessed February 20, 2014).

Im, G., & Rai, A. (2008). Knowledge Sharing Ambidexterity in Long-Term Interorganisational Relationships. *Management Science 54* (7), 1281-1296.

Initiative, U. H. (2012). Exploring Ukrane It Outsourcing Industry 2012.

Ivancevich, D., Hermanson, D., & Smith, L. (2001). The association of perceived disaster recovery plan strength with organisational characteristics. *Journal of information systems*, *12* (1), 31-40

Jarzabkowski, P. A., Le, J. K. & Feldman, M. S. (2012). Toward a Theory of Coordinating: Creating Coordinating Mechanisms in Practice. *Organisation Science. 23*(4), 907-927.

Johnson, I. (2005). The impact on libraries and archives in Iraq of war and looting in 2003: a preliminary assessment of the damage and subsequent reconstruction efforts. *The International Information & Library Review*. *37* (3), 209-71.

Kaplan, M.A., & Haenlein, M. (2010). Users of the World, Unite! The Challenges and Opportunities ofSocial Media. *Business Horizons 53* (1), 59-68.

Kaur, T. (2009). Disaster planning in university libraries in India: a neglected area. *New Library World*, *11*(4), 175-87.

Ketterer, J. J., & Price, B. J. (2006). After the disaster, can you rescue your data?. *The Journal for the Advancement of International Education*. *33*(103), 8-9.

Kgakatsi, I., & Rautenbach, C. J., (2013). The contribution of seasonal climate forecasts to the management of agricultural disaster-risk in South Africa. *International Journal of Disaster Risk Reduction*, *8*, 100–113.

King, J. (2008). Premier 100 Best in Class: Verizon Wireless. *Computerworld*, September 8 (http://www.computerworld.com/ s/article/324221/The_Power_of_One).

King, J. L. (2013). Balance of trade in the marketplace of ideas. *Journal of the Association for Information Systems*, *14*(4).

Klein, R., & Rai, A. (2009). Inter-firm Strategic Information Flows in Logistics Supply Chain Relationships. *MIS Quarterly*, *33*(4), 735–762.

Kline, R. B. (2005). *Principles and practice of structural equation modeling*. New York: The Gilford press.

Kohli, R. (2007). Innovating to Create IT-Based New Business Opportunities at United Parcel Service. *MIS Quarterly Executive*, *6*(4), 199-210.

Kovacs, G., & Spens, K. (2007). Humanitarian Logistics in Disaster Relief Operations. *International Journal of Physical Distribution & Logistics Management*, *37*(2), 99–114.

Lee Y., & Larsen K. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information*, *18*(2) 177-187.

Lee, J., & Berente, N. (2012). Digital innovation and the division of innovative labor: A dual-hierarchy view of complex product architectures. *Organisation Science*, *23*(5), 1428-1447.

Lee, J.Y., & Panteli, N. (2010). Business Strategic Conflict in Computer-Mediated Communication. *European Journal of Information Systems*, *19*(2), 196–200.

Lee, Y. (2010). Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. *Decision Support Systems*, *50*, 361–369

Leidner, D. E., Pan, G., & Pan, S. (2009). The Role of IT in Crisis Response: Lessons from the SARS and Asian Tsunami Disasters. *Journal of Strategic Information Systems*, *18*(2), 80–99.

Leonardi, P. M. (2011). When flexible routines meet flexible technologies. *MIS Quarterly*, *35*(1), 147-167.

Levina, N., & Vaast, E. (2005). The Emergence of Boundary Spanning Competence in Practice: Implications for Implementation and Use of Information Systems. *MIS Quarterly 29*(2), 335-363.

Levitt, A. M. (1997). Disaster Planning and Recovery: A Guide For Facility Professionals ,Wiley, New York, p.1997.

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. Beverly Hills, CA: Sage.

Little, R. (2010). Closed Copter Zone Was Supposed to Allow Medical Flights: 'Miscommunication' Stalls Comfort's Pickup of Quake Victims", *The Baltimore Sun*, January 25, 2010. http://articles.baltimoresun.com/2010-01- 25/news/bal-md.haiti25jan25_1_palace-grounds-flights-helicopters (current Jan. 15, 2014).

Luo, Y. (2007). Are Joint Venture Partners More Opportunistic in More Volatile Environments?. *Strategic Management Journal*, *28*(1), 39–60.

Lwin, M., & Saw, S. (2007). Protecting children from myopia: A PMT perspective for improving health marketing communications. *Journal of Health Communication*, *12*(3), 19-25.

Maitland, C., Tchouakeu, L. & Tapia, A. (2009). Information Management and Technology Issues Addressed by Humanitarian Relief Coordination Bodies" in J. Landgren and S. Jul. (eds.) *Proceedings of the 6th International ISCRAM Conference*, Gothenburg, Sweden.

Majchrzak, A., Jarvenpaa, S., & Hollingshead, A. B. (2007). Coordinating expertise among emergent groups responding to disasters. *Organisation Science, 18*(1), 147-161.

Marincioni, F. (2008). Information Technologies and the Sharing of Disaster Knowledge: The Critical Role of Professional Culture. *Disasters 31*(4) 459-476.

Mete, H.O. & Zabinsky, Z. (2010). Stochastic Optimization of Medical Supply Location and Distribution in Disaster Management. *International Journal of Production Economics*, *126*(1), 76–84.

Miller, P. (2010). The Smart Swarm: How Understanding Flocks, Schools, and Colonies Can Make Us Better at Communicating, Decision Making, and Getting Things Done, New York: Avery.

Mithas, S., & Jones, J. L. (2007). Do Auction Parameters Affect Buyer Surplus in E-Auctions for Procurement?. *Production and Operations Management, 16*(4), 455-470.

Mullan, B. & Wong, C. (2010). Predicting breakfast consumption: An application of the theory of planned behaviour and the investigation of past behaviour and executive function. *British Journal of Health Psychology, 14*(3), 485-504.

Muller, M., & Chua, S. (2012). Brainstorming for Japan: Rapid Distributed Global Collaboration for Disaster Response, *In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '12)*, May 5- 10, New York, NY, USA, ACM Press, 2727-2730.

Nawaz, A. I., & Zualkernan, I. A. (2009) "The role of agile practices in disaster management and recovery: a case study". In Proceedings of the 2009 Conference of the Center for Advanced Studies on Collaborative Research. ACM. 164-173.

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). New York: McGraw-Hill.

Orlikowski, W. J. (2007). Sociomaterial practices: Exploring technology at work. *Organisation Studies, 28*(9), 1435-1448.

Outhwaite, W. (1983). Toward a realist perspective. *Beyond Method: Strategies for Social Research*, 321-330, in G. Morgan (ed.), Sage, Beverly Hills.

Paul, S., & Nazareth, D. (2010). Input Information Complexity, Perceived Time Pressure, and Information Processing in GSS-based Work Groups: An Experimental Investigation Using a Decision Schema to Alleviate Information Overload Conditions. *Decision Support Systems, 49*(1), 31–40.

Philpott, D. (2007). Emergency Preparedness Communications. *Homeland Defense Journal*, *5*(6), 44.

Plotnikoff, R. C., & Higginbotham, N. (1998). Protection motivation theory and the prediction of exercise and low-fat diet behaviours among Australian cardiac patients, *Psychology & Health*, *13*, 411-429.

Plotnikoff, R. C., & Higginbotham, N. (1995). Predicting low-fat diet intentions and behaviours for the prevention of coronary heart disease: An application of protection motivation theory among an Australian population. *Psychology & Health*, *10*, 397-408.

Plotnikoff, R. C., & Higginbotham, N. (2002). Protection Motivation Theory and exercise behaviour change for the prevention of heart disease in a high-risk, Australian representative community sample of adults. *Psychology, Health and Medicine*, *7*(1), 87-98.

Pokharel, S. (2011). "Stakeholders' Roles in Virtual Project Environment: A Case Study," *Journal of Engineering & Technology Management* 28(3), 201-214.

Raju, E., & Niekerk, D. (2013). Intra governmental coordination for sustainable Disaster Recovery: A case study of the Eden District Municipality, South Africa. *International journal of Disaster Risk Reduction*, *4*, 92-99.

Ramchand, A., & Pan, S. (2012). The Co-Evolution of Communities of Practice and Knowledge Management in Organisations. *SIGMIS Database 43*(1), 8-23.

Ramingwong, S., & Sanjeev, A. (2007). Offshore Outsourcing: The Risk of Keeping Mum. *Communications of the ACM, 50*(8), 101-103.

Ramsaran, C. (2005). Running ahead of the pack. *Bank Systems & Technology*, *1*(4), 1-3.

Reuter, C., Heger, O., & Pipek, V. (2012). Social Media for Supporting Emergent Groups in Crisis Management. *Proceedings of CSCW' 12,* February 11–15, 2012, Seattle, Washington, USA.

Rice, D. (2012). 2011 was costliest year in world disasters, USA Today, (http://www.usatoday.com/weather/news/extremes/story/2012-01-04/world-disasters-costliestearthquake tsunami/52377642/1, accessed February 28, 2014).

Robb, D. (2005). Computerworld: Disaster Recovery: Are you ready for trouble? Retrieved August 18, 2013 from the World Wide Web: http://www.computerworld.com/securitytopics/ security/recovery/story/0,10801,101249p3,00.html

Robson, C. (1993). *Real World Research*. Oxford, Blackwell

Romano, N. C., Pick, J & Roztocki, N. (2010). A Motivational Model for Technology-Supported Cross organisational and Cross-border Collaboration. *European Journal of Information Systems*, *19*(2), 117-133.

Rottman, J. W. (2008). Successful Knowledge Transfer within Offshore Supplier Networks: A Case Study Exploring Social Capital in Strategic Alliances. *Journal of Information Technology*, *23*(1), 31- 43.

Saccomanno, P., & Mangialardi, V. (2008). Be prepared for IT disasters. *Canadian Consulting Engineer*, *32*(4), 35-40.

Sagun, A., Bouchlaghem, D., & Anumba, J. C. (2008). A Scenario-based Study on Information Flow and Collaboration Patterns in Disaster Management. *Disasters* *33*(2), 214-238.

Salger, F., & Engels, G. (2010). Knowledge Transfer in Global Software Development: Leveraging Acceptance Test Case Specifications. *ACM/IEEE 32nd International Conference on Software Engineering*, Cape Town, South Africa, 211-214.

Sarker, S., Sarker, S. & Sidorova, A. (2006). Understanding Business Process Change Failure: An Actor-Network Perspective", *Journal of Management Information Systems*, *23*(1), 51 – 86.

Saunders, M., Lewis, P., & Thornhill, A. (2000). *Research methods for business students*,2nd edition. Harlow: Pearson Education.

Sawyer, S., & Winter, S. (2011). Special issue on futures for research on IS: Prometheus unbound? (Editorial). *Journal of Information Technology*, *26*(2), 94-98.

Schubert, P., & Legner, C. (2011). B2B Integration in Global Supply Chains: An Identification of Technical Integration Scenarios. *Journal of Strategic Information Systems*, *20*(3), 250–267.

Schulz, S. F., & Lecken, A. (2010). Horizontal Cooperation in Disaster Relief Logistics: Benefits and Impediments. *International Journal of Physical Distribution & Logistics Management*, *40*(8), 636–656.

Schwalbe, K. (2010). Information Technology Project Management 6th Edition. Course Technology Cenage Learning Boston, MA.

Sedera, D., & Gable, G. G. (2010). Knowledge Management Competence for Enterprise System Success. *The Journal of Strategic Information Systems, 19*(4), 296-306.

Shaheen, M. (2008). Earthquake effects on educational institutions and libraries of Azad Kashmir: an appraisal. *Library Review, 57*(6), 449-560.

Shaluf, I. (2007). An overview on disasters. *Disaster Prevention and Management, 16* (5) 687-703.

Shropshire, J., Kadlec, K. (2009). Developing the IT disaster recovery planning construct. *Journal of Information Technology Management, 20*(4), 233-235

Sieglar,K., & Gaughan, B. (2008). A practical approach to Green IT. Webinar, Retrieved August 18, 2013 from the worldwide web http://www.itmanagement.com/land/green-it-webinar/?tfso=2058

Simchi-Levi, D. (2008). *Designing and Managing the Supply Chain. Concepts, Strategies and Case Studies, 3rd edition*, New York, NY: McGraw-Hill.

Slaughter, S., & Kirsch, L. (2013). Managing the unmanageable: How IS research can contribute to understanding the management of cyber projects. *Journal of the Association for Information Systems*, *14*(4).

Souliotis K., & Papadakis M. (2007). Politics and economics of health. Papazisis. (In Greek).

Stanley M. A., & Maddux J. E. (1986). Cognitive processes in health enhancement: Investigation of a combined protection motivation and self-efficacy model, *Basic and Applied Social Psychology*, *7*, 101-113.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, *22* (4), 441-469.

Sutton, J. (2009) *Twitter service part of disaster communications*, (http://www.canadiansecuritymag.com/Risk-Management/News/Twitter-service-part-of-disastercommunications. html, accessed February 20, 2014).

Tabachnick, B. G., & Fidell, L. S. (2001). Using Multivariate Statistics (4th ed.). Boston, MA: Allyn and Bacon.

Tamura, H., Yamamoto, K., Tomiyama, S., & Hatono, I., (2000). Modeling and analysis of decision making problem for mitigating natural disaster risks. *European Journal of Operational Research, 90* (3), 461–468.

Thomas, A. S., & Kopczak, L. (2007). Life-saving Supply Chains—Challenges and the Path Forward" in H. L. Lee and C. Y. Lee (eds.) *Building Supply Chain Excellence in Emerging Economies*, New York, NY: Springer.

Tilson, D., Lyytinen, K., & Sørensen, C. (2010). Digital infrastructures: The missing IS research agenda. *Information Systems Research, 21*(4), 748-759.

Tiwana, A. (2012). Novelty-knowledge alignment: A theory of design convergence in systems development. *Journal of Management Information Systems, 29*(1), 15-52.

Tiwana, A., Konsynski, B., & Bush, A. A. (2010). Platform evolution: Coevolution of platform architecture, governance, and environmental dynamics. *Information Systems Research, 21*(4), 675-687.

Wakolbinger, T., & Toyasaki, F. (2011). Impacts of Funding Systems on Humanitarian Operations" in M. Christopher and P. Tatham (eds.) *Humanitarian Logistics: Meeting the Challenge of Preparing for and Responding to Disasters*, London, England: Kogan Page, pp. 33–46.

Wall, R., Devine-Wright, P., & Mill, G. A. (2007). Comparing and combining theories to explain proenvironmental intentions: the case of commuting-mode choice. *Environment and behavior*, *39* (6), 731-753.

Walsham, G., & Sahay, S. (2005). Research on information systems in developing countries: current landscape and future prospects. *Information Technology for Development, 12*(1) 7-24.

Warnasuriya, D. (2005). When the tsunami struck Sri Lanka. *Library Hi Tech News, 22* (2), 21-22.

Weaver-Meyers, P., Stolt, W., & Kowaleski, B. (1998). Controlling mold on library materials with chlorine dioxide: an eight-year case study. *The Journal of Academic Librarianship, 24*(6), 455-8.

White, C. M. (2011). *Social Media, Crisis Communication, and Emergency Management: Leveraging Web 2.0 Technologies, USA: Taylor and Francis group.*

Williams, C. (2011). Client–Vendor Knowledge Transfer in Is Offshore Outsourcing: Insights from a Survey of Indian Software Engineers. *Information Systems Journal, 21*(4), pp 335-356.

Workman, M., Bommer, H., & Straub D. (2008). Security lapses and the omission of information security measures: a threat control model and empirical test. *Computers in Human Behavior*, *24*, 2799-2816.

Wurtele, S. K., & Maddux, J. (1987). Relative contributions of Protection Motivation Theory components in predicting exercise intentions and behavior. *Health Psychology*, *6*, 453–466.

Yoo, Y. (2010). Computing in everyday life: A call for research on experiential computing. *MIS Quarterly*, *34*(2), 213-231.

Zu, X., & Kaynak, H. (2012). An Agency Theory Perspective on Supply Chain Quality Management. *International Journal of Operations & Production Management 32*(4), 423-446.

APPENDICES

Appendix A: Questionnaires

NB: *A disaster is a serious disruption in a community or a society causing material, economic, social or environmental losses that go beyond the ability of the affected society to cope using its own resources. These disruptions (disaster) can therefore prevent organisations from reaching their full potential in the provision of goods and services.*

The bearer of this questionnaire is a student of the University of Ghana Business School pursuing MPhil Management Information Systems (MIS). He is conducting a survey on information systems disaster recovery planning in the financial industry in Ghana: the role of management. Please kindly respond to the following questions for the student. Your responses will be duly appreciated and treated with utmost confidentially.

Background information

1. Name of company……
2. Name of person (optional)……..
3. Your position in your organisation……..
4. Which department are you in, please specify……..
5. Gender: a. Male b. Female
6. Age: a. less than 18 b. 18-24 c. 25-30 d. 31-35 e. 36-40 f. Greater than 40
7. Education: a. High school b. Bachelor's degree c. Master's degree d. PHD e. Professional degree f. Others, please specify……
8. How many years have you worked with the organisation: a. 1-5 years b. 6-10 years c. 11-15 years d. over 15 years

Disaster Awareness

9. How do you understand disaster
   ……
   ……
   ……
   ……
   ……
   ……
   ……
10. Are you aware of your organisation's disaster recovery plan a. Yes b. No
11. Which of the following do you regard as a disaster, please tick against the box were applicable

A disaster is a serious disruption in a community or a society causing material, economic, social or environmental losses that go beyond the ability of the affected society to cope using its own resources	
Disaster is an activity which causes severe hazard impact, damage, casualties and disruptions to the population.	
A disaster is the combination of hazard and vulnerability with insufficient capacity to reduce the potential chances of risk	
Disaster is a social crisis situation, a deadly event, usually unexpected and unanticipated and cause human suffering	

Perceived Vulnerability

This factor measures your organisations assessment of the probability of threatening events.

12. Please indicate how much you agree or disagree with each of the following statements:

	Strongly Disagree	Disagree	Neutral	Agree	Strongly agree
I know my organisation could be vulnerable to information systems disaster if we don't put measures in place to combat the disaster	1	2	3	4	5
My organisation information systems could fall victim to disaster if we fail to develop and implement a disaster recovery plan.	1	2	3	4	5
I believe that trying to protect our organisation's information systems will reduce the impact of disaster on it.	1	2	3	4	5
The likelihood of an information system disaster occurring at our workplace is high	1	2	3	4	5

Perceived Severity

This factor measures the severity of the consequences of an event.

13. Please indicate how much you agree or disagree with each of the following statements:

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I believe that planning for disaster for our organisation's information system is important	1	2	3	4	5
Having disaster successfully attack and damage our information system is harmful	1	2	3	4	5
Disaster threats to the security of our organisation's information systems are harmful	1	2	3	4	5
Loss of information systems resulting from disaster is a serious problem for our organisation	1	2	3	4	5
In terms of disaster risks at work, the vulnerability of our information system is low	1	2	3	4	5

Response Cost

This factor emphasizes the perceived opportunity costs in terms of monetary, time, effort expended in developing an information system disaster recovery plan.

14. Please indicate how much you agree or disagree with each of the following statements:

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
There are too many overhead costs associated with developing information systems disaster recovery plan in our organisation.	1	2	3	4	5
Enabling information system disaster recovery plan measures in our organisation is/would be time consuming.	1	2	3	4	5
The inconvenience of developing recommended information system disaster recovery plan measures is lower than the benefits	1	2	3	4	5
The cost of developing an information system disaster recovery plan measures is lower than the benefits	1	2	3	4	5

Response efficacy

This factor relates to the belief about the perceived benefits of the action taken by your organisation.

15. Please indicate how much you agree or disagree with each of the following statements:

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Enabling DRP measures at our workplace will prevent disaster from gaining access to our information systems.	1	2	3	4	5
At our workplace, efforts to ensure the safety of our confidential information from disaster are effective	1	2	3	4	5
The effectiveness of available measures to protect our organisation's information systems from disasters are effective	1	2	3	4	5
The preventative measures available to stop disaster from gaining access to our organisation's information systems are adequate	1	2	3	4	5

Organisational efficacy

This factor emphasizes your organisation's ability or judgment regarding its capabilities to cope with or perform the recommended behavior.

16. Please indicate how much you agree or disagree with each of the following statements:

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
My organisation has the necessary skills to protect its IS from disaster	1	2	3	4	5
My organisation has the expertise to develop preventative measures to stop disaster from getting our information systems	1	2	3	4	5
My organisations ability to prevent IS disaster at my workplace is adequate	1	2	3	4	5

Attitude towards developing ISDRP

17. Please indicate how much you agree or disagree with each of the following statements:

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Developing an ISDRP for our organisation is a good idea	1	2	3	4	5
Developing an ISDRP for our organisation is a necessity	1	2	3	4	5
Developing an ISDRP for our organisation is beneficial	1	2	3	4	5
Developing an ISDRP for our organisation is pleasant	1	2	3	4	5

Subjective norms

Subjective norms are normative stimuli, beliefs and motivations to comply with a particular act, which is largely informed by consultation or observation of the behaviors of others.

18. Please indicate how much you agree or disagree with each of the following statements:

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
My boss thinks that I should develop the organisation's information system disaster recovery plan measures	1	2	3	4	5
My colleagues from other departments think that I should develop the organisation's information system disaster recovery plan measures	1	2	3	4	5
My subordinates think I should develop the organisation's information system disaster recovery plan measures	1	2	3	4	5
I think I should develop an information system disaster recovery plan in order to remain competitive	1	2	3	4	5
I think I should develop an information system disaster recovery plan as required by regulators in the industry	1	2	3	4	5

Perceived behavioral control

Perceived Behavior Control represents an individual's perceived ease or difficulty of performing a particular behavior.

19. Please indicate how much you agree or disagree with each of the following statements:

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
For me participating in developing an ISDRP would be easy	1	2	3	4	5
I feel competent enough to participate in the development of ISDRP	1	2	3	4	5
I am confident of complying to the measures in developing an ISDRP for my organisation	1	2	3	4	5

Motivation and intension for developing a DRP

20. Please indicate how much you agree or disagree with each of the following statements:

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
It is managements intention to continue to develop information system disaster recovery plan	1	2	3	4	5
We would follow the organisation's information system disaster recovery plan	1	2	3	4	5
We shall follow the organisation's information system disaster recovery plan in the future	1	2	3	4	5
We will comply with the organisation's information system disaster recovery plan to protect the organisation's information systems	1	2	3	4	5

Appendix B: Methodology for the Literature Review

Because the initial developments within this research field have been heavily influenced by the activities of practitioners, this literature review incorporates both 'academic' sources (peer reviewed journals, conference papers) and 'practitioner' sources (exclusively non-peer reviewed journal articles, conference papers and other occasional and published papers). A number of criteria were set for the identification, selection and classification of literature sources.

First, it was decided that the review would be time limited. The said review encompasses ISDRP literature published between 2007 and 2013 in a diversity of IS journals. Given ISDRP area of practice and research, this timeframe allowed for the identification of some influential early studies as well as the bulk of recent studies that have appeared in the past six to seven years. Previous review on ISDRP ended on the year 2006 therefore starting from 2007 to 2013 was ideal to continue from the where the previous review ended and also to know the trends and changes that have occurred since that time.

Second, the scope of the review would need to be focused within the IS discipline. The rationale behind this is to know what has been done on DRP within the said discipline. Articles/literature were therefore drawn from a spectrum of IS journals.

Third, the type of content surveyed was limited in terms of the extent to which the research article addressed ISDRP as a defined research area. Only articles dealing with IS, DRP and security as a core issue were included in the review. Thus, search criteria cross referenced key words linked to: a) information systems with b) disaster recovery planning and c) those linked with organisations.

Methodological approaches for the review were classified along qualitative and quantitative. This distinguishes between: a) quantitative studies which tend to be more representative in terms of sampling, but possibly contribute less to theoretical understanding; b) qualitative studies which largely focus on analysis of individual case studies, which make no claims to the general population, but tend to provide more in-depth data concerning processes and contribute more to theory. Also added to this list as suggested by Walsham and Sahay (2005) were: c) mixed methods studies; and d) studies that were purely descriptive.

In conducting the analysis of the articles, the method adopted by the researcher was as follows. In the primary phase, the researcher identified 200 research articles and reports drawn from sources focused on information technology, information systems and computer science. The researcher identified articles which have to be eliminated due to the fact that they were reports and book reviews articles. Others were also duplicate articles. A final sample of 178 was agreed upon for inclusion in the review.

Distribution of articles in journal used for this review

The table below summarizes the sources of the 178 articles that were included in the review together with their date of publication.

	2007	2008	2009	2010	2011	2012	2013	Total
European Journal of Information Systems	2	3	2	2	3	1	2	15
Information Systems Journal	1	3	2	4	4	3	2	19
Information Systems Research	4	5	5	4	3	3	4	28
Journal of AIS	3	4	3	1	1	2	4	18
International Journal of Information security	4	3	5	5	6	3	4	30
Journal of Information Technology	4	4	3	4	3	4	1	23
Journal of MIS	2	2	3	1	2	1	3	14
Journal of Strategic Information Systems	3	4	3	3	4	2	2	21
MIS Quarterly	1	2	1	1	2	2	1	10
Total articles reviewed	24	30	27	25	28	21	23	**178**

From the distribution table above, the highest number of articles for the review was obtained from the international journal of information security which summed up to 30 from the period of 2007 to 2013. The least papers for the review for the same time frame were downloaded from the MIS quarterly.

Appendix C: List of some reference

Ahmed, A. (2011). Use of social media in disaster management use of social media in disaster management. Thirty Second International Conference on Information Systems, Shanghai 2011. [31]

Aziz, Z., Pena-Mora, F., Chen, A., & Lantz, T.(2009). Supporting urban emergency response and recovery using RFID-based building assessment. *Disaster Prevention and Mgmt, 18* (1), 35-48. [45]

Balcik, B., Beamon, M., Krejci, K.M., & Ramirez, M. (2010). Coordination in Humanitarian Relief Chains: Practices, Challenges and Opportunities", *International Journal of Production Economics*, *126*(1), 22–34. [2]

Beggan, D. (2011). Disaster recovery considerations for academic institutions. *Disaster Prevention and Management, 20* (4), 413-422. [42]

Bharosa, N., Lee, J & Janssen, M. (2010). Challenges and Obstacles in Sharing and Coordinating Information during Multi-agency Disaster Response: Propositions from Field Exercises. *Information Systems Frontiers*, *12*(1), 49–65. [22]

Busquets, J. (2010). Orchestrating Smart Business Network Dynamics for Innovation. *European Journal of Information Systems*, *19*(4), 481–493. [16]

Chen, R.,. Rao, H. R, Sharman, R., Upadhyaya, S. J & Kim, J. (2010). An Empirical Examination of IT-enabled Emergency Response: The Cases of Hurricane Katrina and Hurricane Rita. *Communications of the Association for Information Systems*, *26*(8), 141–156. [12]

Clitherow, D., Brookbanks, M., Clayton, N., & Spear, C. (2008). Combining high availability and disaster recovery solutions for critical IT environments. *IBM Systems Journal*, *47* (4) 563-575. [43]

Crowe, A. (2010). The Social Media Manifesto: A Comprehensive Review of the Impact of Social media on Emergency Management. *Journal of Business Continuity & Emergency Planning*, *5*(1), 409 – 420. [14]

Day, J. M., Junglas, M., & Silva, L. (2009). Information Flow Impediments in Disaster Relief Supply Chains. *Journal of the Association for Information Systems*, *10*(8), 637–660. [7]

Erskine, M., Kalantar, H., & Sibona, C. (2013). Aggregating, Analyzing, and Diffusing Natural Disaster Information: A Research Framework. *Proceedings of the Nineteenth Americas Conference on Information Systems*, *Chicago, Illinois,* August 15-17, 2013. [32]

Gao, Y. (2011). Philanthropic Disaster Relief Giving as a Response to Institutional Pressure from China", *Journal of Business Research, 64*(12), 1377–1382. [13]

Guster, C., Brandon, P., & Olivia F. (2008). Cost Effective, Safe and Simple Method to Provide Disaster Recovery for Small and Medium Sized Businesses. *Review of Business Research, 8*(4), 63-71. [19]

Hill, Jeffrey (2008). Business Continuity: Implementing Disaster Recovery Strategies and Technologies. Aberdeen Benchmark Report, March, 2008. [27]

Hiltz, S. R., Van de Walle, B., & Turoff, M. (2010). The domain of emergency management information. *Information Systems for Emergency Managemen*t, Armonk, NY, M.E. Sharpe, 3-20. [24]

Hoffman, D. L., & Novak, P.T. (2012). Need Satisfaction from Interacting with People versus Content: The Roles of Motivational Orientation and Identification with Social Media Groups," (http://ssrn.com/abstract=1990005, accessed February 19, 2014). [26]

Ifinedo, P. (2012). Understanding information systems security policy compliance:An integration of the theory of planned behavior and the protection motivation theory. *computers & security, 3*, 183 – 195. [2]

Iyer, R., & Bandyopadhyay, K. (2000). Managing technology risks in the healthcare sector: disaster recovery and business continuity planning. *Disaster Prevention and Management, 9* (4), 257-270. [33]

Junglas, I., & Ives, B. (2007). Managing IT in a Disaster: Lessons from Hurricane Katrina. *MIS Quarterly Executive*, *6*(1). [23]

Kaplan, M. A., & Haenlein, M. (2010). Users of the World, Unite! The Challenges and Opportunities of Social Media. *Business Horizons, 53*(1), 59-68. [11]

Kendall, K.E., Kendall, J. E., & Lee, K. C. (2006). Understanding Disaster Recovery Planning through a Theatre Metaphor: Rehearsing for a Show that Might Never Open. *Communications of the Association for Information Systems*, *16*(51), 1001-1012. [10]

Lee, J., Bharosa, N., Yang, J., Jassen, M., & Rao, H. (2011). Group value and intention to use - A study of multi-agency disaster management information systems for public safety. *Decision Support Systems 50,* 404–414. [24]

Lee, J. Y., & Panteli, N. (2010). Business Strategic Conflict in Computer-Mediated Communication. *European Journal of Information Systems*, *19*(2), 196–208. [5]

Leidner, D. E., Pan, G., & Pan, S. L. (2009). The Role of IT in Crisis Response: Lessons from the SARS and Asian Tsunami Disasters. *Journal of Strategic Information Systems*, *18*(2), 80–99. [41]

Majchrzak, A., Jarvenpaa, S & Hollingshead, A. (2007). Coordinating Expertise among Emergent Groups Responding to Disasters. *Organisation Science, 18*(1), pp. 147–161. [37]

Marjanovic, O., & Hallikainen, P. (2013). Disaster Recovery – New Challenges and Opportunities for Business Process Management Research and Practice. *Pacific Asia Journal of the Association for Information Systems, 5*(1), 23-44. [54]

Mendonca, D., Jefferson, T., & Harrald, J. (2007). Collaborative Adhocracies and Mix-and-Match Technologies in Emergency Management. *Communications of the ACM, 50*(3), 44–49. [18]

Mills, A., Chen, R., Lee, J. & Rao, H.R. (2009). Web 2.0 Emergency Applications: How useful can Twitter be for emergency response?. *Journal of Information Privacy & Security, 5*(3), 3–26. [15]

Nelson, K. (2007) A Contingency Model of IT Disaster Recovery Planning. *AMCIS 2007 Proceedings.* [1]

Preece, G., Shaw, D., & Hayashi, H. (2013). Using the Viable System Model (VSM) to structure information processing complexity in disaster response. *European Journal of Operational Research,* 224, 209–218. [57]

Shao, B. (2007). Allocating Redundancy to Critical Information Technology Functions for Disaster Recovery. *Proceedings of the Tenth Americas Conference on Information Systems, New York, New York, August 2004*. [51]

Stephens, K. K., Malone, P. C., & Bailey, C. M. (2005). Communicating with Stakeholders during a Crisis. *Journal of Business Communication, 42*(4), 390-419. [25]

Thevenaz, C., & Resodihardjo, S. L. (2010). All the Best Laid Plans…Conditions Impeding Proper Emergency Response. *International Journal of Production Economics*, *126*(1), 7–21. [17]

Van de Walle, B., Turoff, M., & Hiltz, S. R. (2010). Information Systems for Emergency Management, M.E. Sharpe Inc., Armonk, NY. [20]

Wakolbinger, T., Fabian, F., & Kettinger, W. (2013). IT-enabled Interorganisational Information Sharing Under Co-opetition in Disasters: A Game-Theoretic Framework *Communications of* the *Association for Information Systems, 33*, 67–80. [21]

White, C., Plotnick, L., Kushma, J. & Hiltz, S. R. (2009). An Online Social Network for Emergency Management. *International Journal of Emergency Management, 6*(3), 369-382. [8].