

Winter 2011

Application of protection motivation theory to study the factors that influence disaster recovery planning: An empirical investigation

Shalini Wunnavar

Follow this and additional works at: <https://digitalcommons.latech.edu/dissertations>

 Part of the [Industrial and Organizational Psychology Commons](#), and the [Organizational Behavior and Theory Commons](#)

**APPLICATION OF PROTECTION MOTIVATION
THEORY TO STUDY THE FACTORS THAT
INFLUENCE DISASTER RECOVERY
PLANNING: AN EMPIRICAL
INVESTIGATION**

by

Shalini Wunnava, B.A., M.B.A.

A Dissertation Presented in Partial Fulfillment
of the Requirements for the Degree of
Doctor of Business Administration

COLLEGE OF BUSINESS
LOUISIANA TECH UNIVERSITY

February 2011

UMI Number: 3451090

All rights reserved

INFORMATION TO ALL USERS

The quality of this reproduction is dependent upon the quality of the copy submitted.

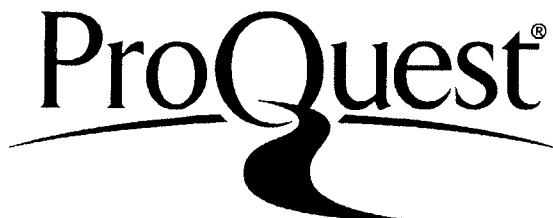
In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if material had to be removed, a note will indicate the deletion.



UMI 3451090

Copyright 2011 by ProQuest LLC.

All rights reserved. This edition of the work is protected against unauthorized copying under Title 17, United States Code.



ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

LOUISIANA TECH UNIVERSITY

THE GRADUATE SCHOOL

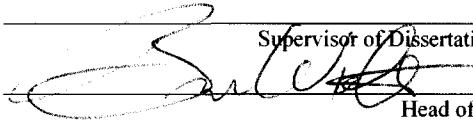
January 6, 2011

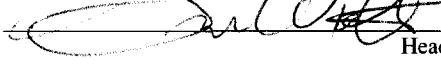
Date

We hereby recommend that the dissertation prepared under our supervision
by Shalini Wunnava

entitled "Application of Protection Motivation Theory to Study the Factors that Influence
Disaster Recovery Planning: An Empirical Investigation"

be accepted in partial fulfillment of the requirements for the Degree of
Doctor of Business Administration - Computer Information Systems

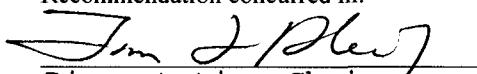
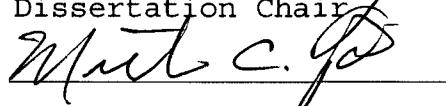
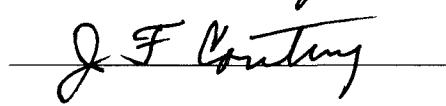

Supervisor of Dissertation Research


Head of Department

Management and Information Systems

Department

Recommendation concurred in:


Dissertation Chair




Dissertation Co-Chair

Advisory Committee

Approved:


Director of Graduate Studies

Approved:


Dean of the Graduate School


Dean of the College

GS Form 13a
(6/07)

ABSTRACT

In today's information intensive and networked world, Disaster Recovery Planning (DRP) is a critical and significant activity. However, DRP does not always receive the attention it deserves. Therefore, it is critical to examine the factors that influence the undertaking of disaster recovery planning. A model on disaster recovery planning was developed using the theoretical lens of Protection Motivation Theory (PMT). Drawing from PMT literature and using the information technology disaster recovery planning (ITDRP) construct developed by Shropshire and Kadlec (2009), a research model was developed in which perceived severity, perceived vulnerability, intrinsic rewards, extrinsic rewards, fear, response efficacy, self-efficacy, and response costs are the determinants of ITDRP. The results of an Exploratory Factor Analysis (EFA) indicated issues of conceptual overlap of items of perceived severity with other factors and therefore, the variable perceived severity was dropped from the model. Based on a Principal Components Analysis (PCA), the items of ITDRP were consolidated into three factors: (1) identification, recovery, and back-up procedures; (2) procedures for the DRP plan, human resources, and physical facilities; and (3) offsite storage. Three regression models were formed with these three factors as the dependent variables. The regression results showed that self-efficacy and response costs were significant and consistent predictors of ITDRP. These results are consistent with previous studies that used PMT in other contexts.

APPROVAL FOR SCHOLARLY DISSEMINATION

The author grants to the Prescott Memorial Library of Louisiana Tech University the right to reproduce, by appropriate methods, upon request, any or all portions of this Dissertation. It is understood that "proper request" consists of the agreement, on the part of the requesting party, that said reproduction is for his personal use and that subsequent reproduction will not occur without written approval of the author of this Dissertation. Further, any portions of the Dissertation used in books, papers, and other works must be appropriately referenced to this Dissertation.

Finally, the author of this Dissertation reserves the right to publish freely, in the literature, at any time, any or all portions of this Dissertation.

Author W.S.Shalini Nag
Date February 2011

DEDICATION

I dedicate this dissertation to my family – my parents, two elder brothers, sister-in-law, niece, and nephew.

Daddy, Mummy, Bablanna, Rajanna, Bhavu, Shreyu, and Rishi...this one is for all of you!!

I love you!!!

TABLE OF CONTENTS

ABSTRACT.....	iii
DEDICATION.....	v
LIST OF TABLES.....	ix
LIST OF FIGURES	x
ACKNOWLEDGEMENTS.....	xi
CHAPTER 1 INTRODUCTION	1
Protection Motivation Theory.....	3
Information Technology Disaster Recovery Planning.....	4
Conceptual Research Model	4
Data Collection and Research Methods.....	6
Organization of Chapters	6
CHAPTER 2 LITERATURE REVIEW	7
Disaster Recovery Planning.....	7
Losses Due to Disasters	11
Absence of a DR Plan: The Impact	12
DRP: A Top Issue	13
Reasons for Lack of DRP	14
Theoretical Application to DRP	15
Protection Motivation Theory.....	16

Revised Model	18
Analysis of PMT	23
Applications of PMT	25
Application of PMT in Health Studies	26
Impact of Health Threat Warnings and Fear Appeals Upon Protective Behavior.....	26
Fear Appeals	27
Impact of Uncertainty Orientation on Protective Behavior	29
Determinants of Non-Compliance	30
Extension of PMT Related Health Studies to Children and Adolescents	30
PMT and Subsequent Behavior	31
Inclusion of Risk into PMT	31
Application of PMT in Information Security Studies.....	32
Model Development and Hypotheses	36
Outcomes of the Model.....	40
CHAPTER 3 RESEARCH METHODS	43
Variables	43
PMT Constructs	43
Determinants of ITDRP	44
Instrument Design.....	46
Scale Computation.....	47
Construct Validity and Reliability	49
Data Collection	50

Statistical Methodology	52
CHAPTER 4 DATA ANALYSIS AND RESULTS	54
Validity and Reliability Assessment.....	54
Checking Assumptions	63
CHAPTER 5 DISCUSSION AND CONCLUSION	73
Summary	73
Implications for IS Theory.....	75
Implications for IS Practice	76
Limitations and Future Research	77
APPENDIX A SURVEY INSTRUMENT	79
APPENDIX B HUMAN USE LETTER	92
REFERENCES	94

LIST OF TABLES

Table 2.1	Schema of the Original Protection Motivation Theory with Self-Efficacy Added	25
Table 2.2	PMT Research, Significance, Theoretical Advancement, and Contextual Application	33
Table 2.3	Hypotheses	42
Table 3.1	PMT Variables	44
Table 3.2	ITDRP Dimensions	45
Table 3.3	Scales	46
Table 3.4	Nature of Constructs and Scale Computation	48
Table 3.5	Respondent Profile	51
Table 4.1	Loadings for PMT Reflective Constructs	55
Table 4.2	Loadings for PMT Formative Constructs	57
Table 4.3	Loadings for ITDRP Constructs	57
Table 4.4	Reliability Analysis for Independent Variables	59
Table 4.5	Reliability Analysis for Dependent Variables	59
Table 4.6	Results of Multiple Regression Analysis	66
Table 4.7	Hypotheses Supported/Not Supported	70

LIST OF FIGURES

Figure 1.1	Conceptual Research Model	5
Figure 2.1	Schema of the Original Protection Motivation Theory.....	18
Figure 2.2	Schema of the Revised Protection Motivation Theory	21
Figure 2.3	Original Conceptual Research Model.....	39
Figure 4.1	Regression Model 1	61
Figure 4.2	Regression Model 2	62
Figure 4.3	Regression Model 3	63
Figure 4.4	Model 1 Hypotheses	67
Figure 4.5	Model 2 Hypotheses	68
Figure 4.6	Model 3 Hypotheses	69

ACKNOWLEDGEMENTS

I wouldn't have achieved this goal and be where I am today, if it were not for the love, support, guidance, and encouragement of a lot of people in my life. I am thankful to my family for their love and support without which I would not have been able to accomplish this.

I have met some really kind and wonderful people in Ruston. People who form my special circle of friends and have helped me weather many a storm in life and have helped to overcome many hurdles. I would like to mention a special thanks to Satish and Deeba for standing by me every step of the way on this journey. Thank you..April, Mridu, Jude, Vivien, Olga, and Dana. I also want to thank my friends Raju, Siri, Kiran, Shanthi, Mangi, Bhabhi, Jinson, Prathi, Sathi, and Vidhi. Mahesh Uncle, Aunty, and Vasu, thank you for making me a part of the family. I would also like to thank my friends from Albany – Buddy, Late Prof. Hughs, Mrs. Hughs, Dr. Bob, Ama, Cathy, Pei Feng, Michele, Viji Mol (Aunty), and Moideen Uncle. A special thanks to Kiran and Jude for taking care of me when I fell sick with pneumonia during the last two months of my dissertation. A special thanks to Ratan who despite being miles away was my constant source of support during the last two months of finishing up my dissertation. I would also like to thank my friends Kamphol, Paul, and Aru.

Being an international student living far from family is not easy, and especially when you fall sick. I thank all my friends, my classmates and colleagues in the doctoral program, professors and staff in the College of Business for their help and support.

I thank my dissertation co-chairs Dr. Roberts and Dr. Ellis for their guidance and support. Dr. Roberts, you repeatedly talked about the importance of theory and the concepts of validity and reliability in your classes, and asked us questions on those in the comps. Little did I know at that time what a solid foundation you were helping us to build in order to develop our research skills. Thank you, Dr. Roberts. Thank You Dr. Ellis for encouraging me to submit my first conference paper, for always being supportive, and for helping me with any campus related issues, especially during the few months I was away from Ruston. I also want to thank my dissertation committee members Dr. Courtney and Clay. Thank you, Dr. Courtney for being on my dissertation committee. Thank you Clay for coming on board in the last minute and offering some valuable advice based on your research expertise and your own recent dissertation experience.

I thank Dr. Cochran and Dr. Mesak for giving me a solid foundation in Quantitative Analysis through their classes. Dr. Cochran, your take home QA exams meant that we had to live and breathe QA. But I loved every moment of it. I learnt so much. Thank you for making QA so much fun. I thank Dr. Pullis for teaching me the significance of a semi-colon in writing, and for being an example of kindness and goodness in life. I thank Dr. Kroll for introducing me to research. I greatly thank Dr. Stephens for teaching me the ropes of research, for making me realize my potential, encouraging me towards my goals, and for being so supportive.

I would also like to thank Dr. Walters, Shawn, Ms. Gantt, Ms. Joyce, and Retired Dean Reagan for their kindness. Shawn, I will always remember about ‘paying it forward’. Thank you. Caroline, thank you for your friendship and for all the help you gave me. Last but not the least; I would like to thank all my classmates and colleagues in the doctoral program for their friendship, camaraderie, and support. Krist, Dr. Bari, Son, Kate, Jim, and Clay -- thank you so much.

I would like to thank Dr. Brantley, Ms. Cindy, Fred and The Eubanks family for their kindness. I also want to thank Mrs. Pullis for the love and the care and for always being there. And a special thanks to Ms. Sandi for helping me with the last stage of my dissertation and the format review process.

I thank God and life for making such wonderful and kind people a part of my life, for filling my life with love, laughter, and happiness, for giving me the strength and opportunities, hopes and dreams, and the work ethic and determination to work towards making my dreams come true.

Daddy, many years back it all started with a dream and today that dream has come true. I know you can see it all from up there. Just want you to know I love you and I miss you and always will.

CHAPTER 1

INTRODUCTION

Disaster recovery (DR) plan deals with the preparation for and recovery from a disaster, irrespective of whether the disaster is natural or human-made (Whitman & Mattord, 2007). The focus of the DR plan is to restore systems at the original site post-disaster (Whitman & Mattord, 2007). In a study of companies that suffered a major data loss and did not have a BC/DR plan, 43% never reopen, 51% close within two years, and only 6% survive in the long run (Cummings, Haag, & McCubrey, 2005; Snedaker, 2007). Mitroff, Harrington, and Gai (1996) state that organizations that prepare for crisis, usually recover three times faster than the unprepared organizations, and also face significantly less financial and human cost. Yet, the Info-Tech Research Group reports that 60% of North American businesses do not have a DR plan (Chisholm, 2008).

Kendall, Kendall, and Lee (2005) state that the present is engaging and planning for disasters seems remote, and some people just dislike the emphasis of negative or emergency scenarios. Kendall et al. (2005) term this approach of firms burying their head in the sand and pretending not to see the impending disaster as the ostrich approach.

Unfortunately, disasters do strike and range from the trivial and familiar (power outages) to the severe and unexpected such as natural disasters (e.g., the 2005 hurricanes Katrina and Rita and, the 2004 tsunami that hit Southeast Asia) or terrorist attacks (World

Trade Center attacks on 9/11, the Bali bombings, the London tube bombings) (Kendall et al., 2005). It is clear that in today's information intensive and networked world, disaster recovery planning is a critical and significant activity. Yet, there have been relatively few studies on pre-disaster planning efforts and IT-oriented disaster recovery planning research is scant (Shao, 2005). This provides further justification that any research on IT-oriented disaster recovery planning that studies the motivations and other influencing factors that lead to the intention to undertake disaster recovery planning would make a value-added contribution to existing research. Moreover, such kind of a research could also provide some additional understanding of why the need for disaster recover planning does not always translate into an equally proportional intention to undertake disaster recover planning.

The application of theoretical frameworks to disaster recovery as such have been very limited, but more so with regard to gaining an understanding into this reluctance and lack of initiatives to undertake DRP. Protection motivation theory (PMT) provides a framework to understand the motivators that lead individuals to undertake protective measures. Adapting the protection motivation theory and applying it to a study on disaster recovery planning could shed new lights on the behavioral factors that underlie the decisions to undertake disaster recovery planning. Therefore, this research includes the development of a conceptual model (Figure 1.1) that is used to study the factors that lead to disaster recovery planning. This research study includes: (1) the development of a conceptual model, (2) survey instrument development to enable data collection for model testing, and (3) empirical testing of the conceptual model. The following sections provide

a brief description of protection motivation theory, and also include definitions of information technology disaster recovery planning (ITDRP).

Protection Motivation Theory

The Protection Motivation Theory states that the motivation of the stakeholders to protect themselves from harm is enhanced by the following four perceptions: (1) the severity of the threat, (2) their vulnerability to the threat, (3) self-efficacy, i.e., their confidence in their ability to cope with the threat and perform threat reducing behaviors, and (4) response efficacy, i.e., the ability of the response to reduce the threat (Maddux & Rogers, 1983; Rogers, 1983). 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 organizations to implement disaster recovery planning.

Information Technology Disaster Recovery Planning

DRP has not received attention in mainstream IS research, which boasts of only 6 articles that were published in peer-reviewed MIS journals in the past ten years (Shropshire & Kadlec, 2009). In order to rectify this, Shropshire and Kadlec (2009) have provided a domain definition of information technology disaster recovery planning (ITDRP) covering seven dimensions, leading to the development of a 34 item measure for assessing the degree of ITDRP. According to the definition by Shropshire and Kadlec (2009), IT disaster recovery planning comprises of the seven dimensions: *IT disaster identification and notification, preparing organizational members, IT services analysis, recovery process, backup procedures, offsite storage, and maintenance*. These seven dimensions represent the collective actions that firms need to take in order to ensure recovery post IT disasters (Shropshire & Kadlec, 2009).

Conceptual Research Model

In this study an effort is made to study disaster recovery planning through the lens of PMT to explain what could be the factors influencing disaster recovery planning in organizations. The conceptual model includes all the PMT constructs as predictors of the over all ITDRP construct. Perceived severity, perceived vulnerability, intrinsic rewards, extrinsic rewards, fear, response efficacy, self-efficacy, and response costs are modeled as the predictors of ITDRP. This conceptual model is depicted in Figure 1.1.

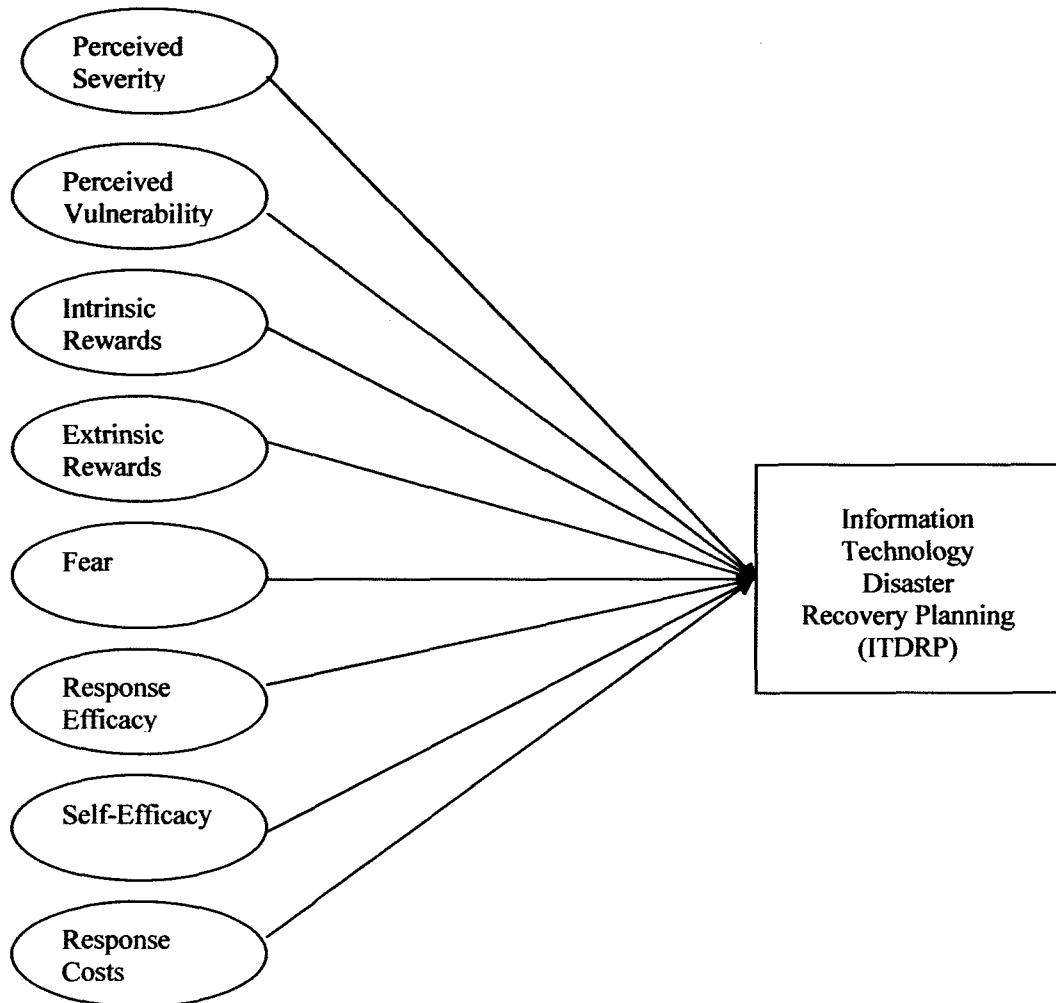


Figure1.1. Conceptual Research Model

It is expected that perceived severity, perceived vulnerability, fear, response efficacy, and self-efficacy will have a significant positive relationship with ITDRP. Intrinsic rewards, extrinsic rewards, and response costs are expected to have a significant negative relationship with ITDRP.

Data Collection and Research Methods

The survey instrument was developed based upon existing scales. For data collection, Zoomerang's panel of IT disaster recovery planning professionals was used. In the initial stages of the study, the inclination was towards using Partial Least Squares (PLS) methodology as it is considered to be appropriate when using formative indicators in the model (Chin, 1998). But further along into the study, and having a sample size of only 184, based on Gefen, Straub, and Boudreau (2000), it seemed more appropriate to use the statistical technique of linear regression for the data analysis. Therefore, the independent/predictor variables were regressed on the three dependent variables separately in three regression models.

Organization of Chapters

This dissertation is organized into five chapters. In this first chapter, the objectives and need for the research have been discussed, along with a brief background of the theoretical constructs used and an introduction to the conceptual model development. Chapter 2 covers the literature review and initial model development. Chapter 3 focuses on the survey instrument, data collection, and research methods. Chapter 4 covers the initial results, model refinement, and final results and their interpretation. And finally, Chapter 5 concludes the dissertation with a discussion of the results, their interpretation and implications, along with the scope for future research.

CHAPTER 2

LITERATURE REVIEW

The introductory chapter served as an overview of this research study, including an introduction to the applied concepts and theories, conceptual model, research methods, and significance of the study. This chapter provides a review of the literature regarding the primary concepts and theories applied in this study. Further, the latter part of the chapter describes the development of the conceptual model.

Disaster Recovery Planning

Toigo (2005) defines Disaster recovery planning (DRP) as the activities that are aimed at reducing the probability and also limiting the impact of disastrous events on critical business processes. Toigo (2000) believes that this simplistic definition may not satisfy those who would like more specific definitions that would differentiate DRP from business continuity planning and other forms of planning, thus suggesting the existence of a semantic debate with regard to the definition of DRP.

Kendall, Kendall, and Lee (2005) define disaster recovery planning (DRP) as a process that supports a firm's ability to recover the core business functionality of its software, data, and systems after the occurrence of a natural or human-made disaster. Cole, Krutz and Conley (2005) define DRP as protecting critical business processes from the effects of major information system and network failures and quickly

recovering from an emergency with a lowest possible impact on the organization. Shao (2005) defines DR plan as a system for internal control and security planning that focuses on speedily restoring critical organizational processes in the event of operational failures due to natural or human-made disasters. The objective of an IT DR plan is to ensure that an organization's computing and communication systems operate smoothly without any interruptions during and after a disaster (Shao, 2005).

There are two problems with all the above definitions. Firstly, the current definitions clearly do not state whether the aim of the DR plan is to just ensure the continued operation of critical functions or specifically a recovery at the original site of disaster. Secondly, these definitions do not distinguish between the overlapping concepts of disaster recovery planning, business continuity, and incident recovery. Whitman and Mattord (2007) make this distinction by clearly delineating between business impact analysis (BIA), disaster recovery planning (DRP), incident recovery planning (IR), and business continuity planning.

A contingency plan includes business impact assessment, incident response planning, disaster recovery planning, and business continuity planning; it is prepared by an organization so that it can not only anticipate, react to, and recover from any security threats facing the information and information assets of the organization, but also restore the organizational operations (Whitman & Mattord, 2007). Whitman and Mattord (2007) define business impact analysis (BIA) as an investigation and evaluation of the impact of various attacks on the organization and involves prioritized lists of threats and vulnerabilities and addition of critical information; further it provides detailed scenarios of potential impact of every possible attack (Whitman & Mattord, 2007). The incident

response plan is the document in which all the actions that an organization can and should take during an incident are defined; and an incident is any clear and defined attack on the organization's information assets that pose a threat to the assets' confidentiality, integrity, and recovery (Whitman & Mattord, 2007). The IR plan deals with the question of "what do I do now?" in the midst of an incident and is an immediate response to an incident, but if the incident escalates or is disastrous in nature such as for instance a fire, flood, earthquake, or a total blackout, then the process moves onto disaster recovery and business continuity (Whitman & Mattord, 2007). The disaster recovery (DR) plan deals with the preparation for and recovery from a disaster; irrespective of whether the disaster is natural or human-made (Whitman & Mattord, 2007).

Although, DR planning and IR Planning might seem similar and overlap to a certain extent, they differ in terms of their urgency and results; and moreover, DR plan is considered to be a subsection of the IR plan that covers disastrous events (Whitman & Mattord, 2007). The focus of the DR plan is to restore systems at the original site post-disaster (Whitman & Mattord, 2007).

The core of disaster recovery planning from a traditional perspective focuses on identifying post-disaster requirements versus how to avoid the disaster in the first place (Buchanan, 2003). Legacy disaster plans include backup (critical data is copied to a removable storage media and stored off-site and this process is repeated regularly), replication (duplicate database is created on a different physical storage media), redundancy (second computer system is available to replace the first in case of a failure), and failover (failure of the primary system is automatically detected by the failover system and recovery is automated) (Buchanan, 2003). Peter Fallara (2003) identified

backup methods, alternate sites, equipment replacement, and support teams to be some of the components of a disaster recovery plan. In some companies, however, backing up data and methods for restoring data resources may constitute disaster recovery planning (Jackson, 2008; Preimesberger, 2008). This indicates that there is no consistent measure as to what constitutes disaster recovery planning, and presents a very important research issue, which will be discussed in further detail towards the end of this section.

Business continuity (BC) plan is a document that details how an organization can ensure the continuation of its critical business functions at an alternate location while the recovery efforts continue at the primary site in case of the occurrence of a catastrophic incident or disaster (Whitman & Mattord, 2007). In addition to end-to-end system availability, business continuity implies the protection of personnel and facilities (Buchanan, 2003). Moreover, in order to ensure business continuity, it is required to take disaster avoidance steps (Buchanan, 2003). Therefore, BCP is a holistic approach to ensuring continued business operations post-disaster (Crowe, 2007; Whitman & Mattord, 2007; Anderson, 2008).

Business continuity planning (BCP) is considered to be a methodology that is used to create and validate a plan for maintaining continuous operation of business not only before, but also during and after disasters and disruptive events (Snedaker, 2007). On the other hand, disaster recovery is considered to be a part of business continuity and is about dealing with the immediate impact of an event, for instance, recovering from a hurricane or a server outage (Snedaker, 2007).

To further clarify the differences between IR, DR, and BC plans, it can be said that when an attack occurs, the incident is detected and IR plan is set in motion. If the

incident is considered just an incident, then the IR plan is carried through, but if the incident is classified as disastrous, the DR plan is set into motion and ends only with restoration of operations at primary site. If the disaster requires any off-site operations, then the BC plan is set into motion and operations are carried on at alternate sites, till the business operations can be restored at the primary site.

Although, based on the preceding discussion, the definition of DRP seems clear and it has been distinguished from BCP, one thing that has not been addressed is how to measure DRP. This lack of a valid measure of DRP pinpoints to the issue that DRP although discussed in text books, has not received attention in mainstream IS research, which boasts of only 6 articles that were published in peer-reviewed MIS journals in the past ten years (Shropshire & Kadlec, 2009). In order to rectify this, Shropshire & Kadlec (2009) have provided a domain definition of information technology disaster recovery planning (ITDRP) covering seven dimensions, leading to the development of a 34 item measure for assessing the degree of ITDRP. According to the definition of Shropshire and Kadlec (2009), IT disaster recovery planning comprises of the seven dimensions: *IT disaster identification and notification, preparing organizational members, IT services analysis, recovery process, backup procedures, offsite storage, and maintenance*. These seven dimensions represent the collective actions that firms need to take in order to ensure recovery post IT disasters (Shropshire & Kadlec, 2009).

Losses Due to Disasters

Hoffer (2001) found that of the companies that had a major loss of computerized data, 43% never reopen, 51% close within two years, and only 6% survive in the long-term. A 2002 U.S. Bureau of Labor study reports that 93% of companies experiencing a

significant data loss go out of business within five years. A more recent study by Gartner, reports that 40% of all small to medium businesses go out business if they cannot access their data in the first 24 hours following a disaster (Rennels, 2006). The U.S. National Fire Protection Agency reports that 43% of companies never resume business after a major fire and another 35% are out of business within 3 years (Rennels, 2006). Whitman and Mattord (2007) found that 80% of businesses affected by a major incident either never reopen or else end up getting closed within 18 months. A Faulkner Information Services research study found that 50% of companies that suffer from data loss due to disasters go out of business within 24 months (Chisholm, 2008).

Absence of a DR Plan: The Impact

Veritas 2004 Disaster Recovery Research reported that the five most likely consequences of a disaster in the absence of any DR plan include: data loss (43%), decreased employee productivity (62%), damage to customer relationships (38%), reduction in profits (40%), and reduction in revenue (27%).

In a study of companies that suffered a major data loss and did not have a BC/DR plan, 43% never reopen, 51% close within two years, and only 6% survive in the long run (Cummings, Haag, & McCubrey, 2005; Snedaker, 2007). A Gartner, Inc. study reported that less than 10% of small and medium businesses had disaster plans, and that 40% of companies that experience a disaster and have no DR plan will go out of business within five years (Snedaker, 2007). Snedaker (2007) points out that 150 of the 350 businesses located in the World Trade Center during the 1993 bombing went out of business, but even after 09/11 a majority of the financial firms located in the twin towers were back in business within two days because they had well-developed and tested BC/DR plans.

DRP: A Top Issue

Mitroff, Harrington, and Gai (1996) found that organizations that prepare for crisis, usually recover three times faster than the unprepared organizations, and also face significantly less financial and human cost. An August 2003 Harris Interactive poll suggested that senior corporate executives in Fortune 1000 companies on an average graded their companies at C-plus when it comes to the organizational ability to ensure information availability post disaster (Anonymous, 2003). A Veritas 2003 Disaster Recovery Research reports that of those surveyed, only six percent feel vulnerable to hurricanes and tornadoes, while 25% feel threatened by terrorism; but, technological failure was ranked the highest perceived threat. According to the Veritas 2003 research report, the top five most common threats faced by large companies include hardware failure (61%), software failure and viruses (both 59%), fire (56%), hackers (36%), and accidental employee error (31%). A 2004 report in Information Week stated that 25% of the surveyed organizations had to bring into play their disaster recovery or business continuity plans in 2003; of these 70% reported the disaster to be severe or extremely severe (Whitman & Mattord, 2007).

The 2008 EDUCAUSE Current Issues Survey ranked disaster recovery/business continuity at sixth position in its list of top 10 information technology (IT) issues for 2008 (Allison & DeBlois, 2008). The 2007 Society for Information Management (SIM) survey ranked continuity planning and disaster recovery fourth in its list of the top-five applications and technologies (Luftman & Kempaiah, 2008).

Reasons for Lack of DRP

Of the Fortune 1,000 companies, less than half have DR plans; of the smaller companies only 15%-20% have plans and further, only 20% of the existing plans were workable (Brunetto & Harris, 2001). Small businesses account for 99% of all employers in the United States, 75% of all new jobs, and 97% of all exporters (Snedaker, 2007). This indicates how important it is even for small businesses to have a DR plan. An August 2002 American Management Association study revealed that more than half of the surveyed companies did not have any disaster recovery or crisis management plan (Snedaker, 2007). The Veritas 2003 Disaster Recovery Research reported that 24% of the companies don't test their DR plans; this figure is even higher in the U.S with a 34% of the companies not testing their DR plans. Lack of time was reported to be the top barrier to testing according to the Veritas 2003 Disaster Recovery Research. The Info-Tech Research Group reports that 60% of North American businesses do not have a DR plan (Chisholm, 2008). An October 2005 survey by the Advertising Council found that 92% of the surveyed business admitted that it is important to plan for emergencies; 88% agreed that it makes sense to have some emergency plan; 39% actually had a plan; but 12% believed that having an emergency plan made no sense (Snedaker, 2007). Despite the losses due to Hurricane Katrina, Farazmand (2007), points out that many firms are still very negligent about DRP.

Despite all the statistics that reveal how being unprepared for disasters could prove to be devastating for businesses, it is shocking that 12% of those surveyed felt that it makes no sense to have an emergency plan of any sort. Using a football analogy to highlight the importance of DRP, Fallara (2003) explained that the best defense is a well

managed offense. Yet, organizations do not take measures to ensure the development, testing, and implementation of DR plans. In order to understand the “why”, theoretical frameworks should be evaluated.

Theoretical Application to DRP

The application of theoretical frameworks to disaster recovery as such have been very limited, but more so with regard to gaining an understanding into this reluctance and lack of initiatives to undertake DRP. Some of the theoretical frameworks found in literature with regard to studies on disaster recovery will be briefly mentioned here.

Herzog (2007) believes that disaster planning/mitigation could benefit from theoretical frameworks. Further, Herzog (2007) lists the theories that should influence disaster planning/mitigation to include chaos, communitarian, critical, cultural, deconstruction, Marxist, populist, pragmatist, rational, and social constructivist. An applied research project by Gatlin (2006) found support for the application of Jane Addam's Social Democratic Theory and Ethics as a theoretical framework for long term disaster recovery efforts. Piotrowski (2006) applied the Chaos Theory to understand the devastation and also organizational dysfunction that was witnessed after Hurricane Katrina. According to the Chaos Theory, crises and human reactions to intense stressors are highly unpredictable, difficult to control, and also they resist effective management and organization attempts (Piotrowski, 2006).

Herzog (2007) specifically believes that theory and planning are related. Planning is nothing, but preparation to reduce the effects of any future event, and theories aid the planners to achieve this goal; therefore, theories can serve as a foundation for planning (Herzog, 2007). Further, planning is considered to be the bridge or connection between

theory and action (Herzog, 2007). Therefore, it can be concluded that there has to be a possible explanation in theory to the research question of why don't organizations undertake DRP, despite knowing the critical significance of it.

Protection motivation theory (PMT) provides a framework to understand the motivators that lead individuals to undertake protective measures. It is believed that this theory could shed some light in understanding the organizational motivations for protective measures such as DRP. Therefore, in the following section PMT will be discussed in detail.

Protection Motivation Theory

Rogers (1975) considers Protection Motivation Theory (PMT) to be connected with the theoretical tradition that uses expectancy-value formulations (also known as means-ends instrumentality theories). Most theoretical formulations used to study social psychological phenomena explain that behavioral tendency is a function of expectancies that the particular act will be followed by a consequence and also the value of the consequence. (Rogers 1975). Using such theoretical expectancy-value formulations, social psychological phenomena such as the structure of attitudes, the prediction of behavior from self-report measures, and persuasion in the health field have been studied.

PMT was proposed to advance the understanding of fear appeals and attitude change (Rogers, 1975). PMT is grounded on the three crucial stimulus variables in a fear appeal: (a) the magnitude of noxiousness of a depicted event; (b) the conditional probability that the event will occur provided that no adaptive behavior is performed or there is no modification of an existing behavioral disposition; and (c) the availability and effectiveness of a coping response that might reduce or eliminate the noxious stimulus

(Rogers, 1975; Hovland et al., 1953). These variables are considered the communication components, each of which is assumed to initiate a cognitive mediation process. This process appraises communication information about noxiousness, probability, or efficacy by placing each stimulus on dimensions of appraised severity of the depicted event, expectancy of exposure to the event, or belief in efficacy of the recommended coping response (Rogers, 1975).

Rogers (1975) points out that these three cognitive processes mediate the effects of the components of fear appeals upon attitudes by arousing “protection motivation”. Furthermore, the intention to adopt the recommended communication is mediated by the protection motivation aroused (Rogers, 1975). Protection motivation is an intervening variable with the typical characteristics of a motive that arouses, sustains, and directs activity (Rogers, 1975) and is operationalized as intentions (Rogers, 1983; Witte, 1992). The model of protection motivation theory as formulated and schematically represented by Rogers (1975) is presented in Figure 2.1.

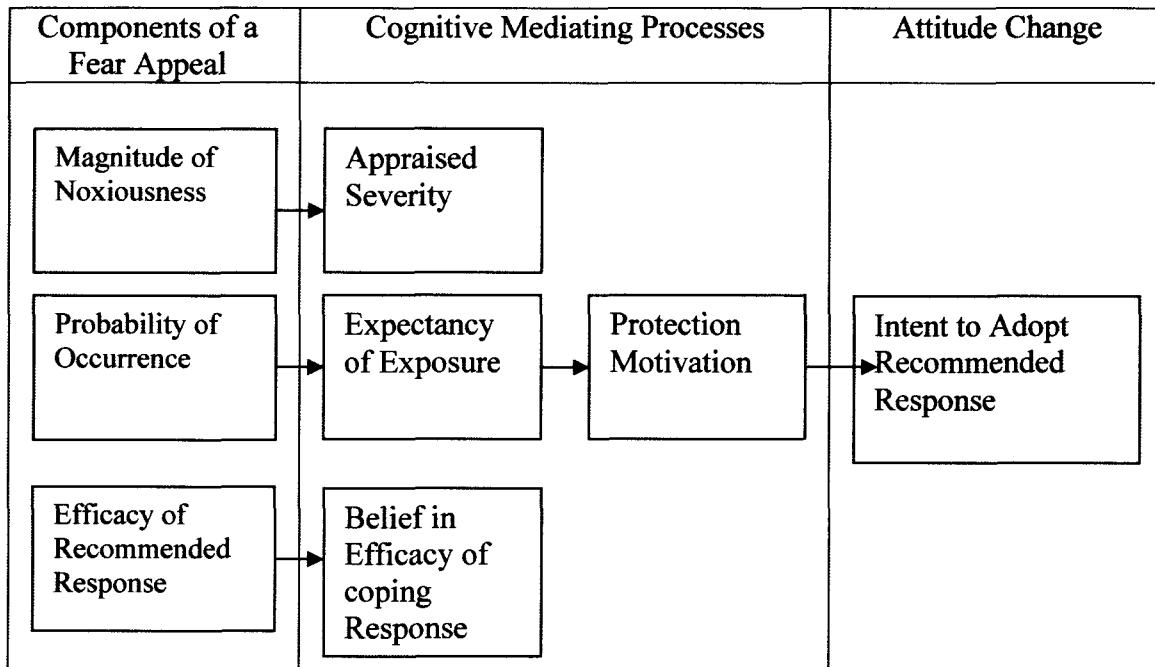


Figure 2.1. Schema of the Original Protection Motivation Theory
Source: Rogers (1975, p.99)

Revised Model

It is not enough to have knowledge of an effective coping response alone in order for a subject to adopt that response; it is also important that the subject also believes in his or her own ability to perform the behavior" (Maddux & Rogers, 1983; Tanner Jr., Day, & Crask, 1989). In the revised version of protection motivation theory, self-efficacy expectancy was included in an attempt to present a more comprehensive model (Rogers, 1983, Maddux & Rogers, 1983). Self-efficacy theory postulates that all processes of psychological change operate through alteration of the individual's expectancies of personal mastery or efficacy. Self-efficacy is an individual's belief that she or he is or is not capable of performing the required behavior (Bandura, 1982; Maddux & Rogers, 1983). The self-expectancy theory states that effective coping can be viewed as two independent expectancies, namely, outcome expectancy and self-efficacy (Maddux &

Rogers, 1983). Outcome expectancy is the belief about whether a given behavior will or will not lead to a given outcome (Maddux & Rogers, 1983). Maddux and Rogers (1983) experimentally manipulated self-efficacy expectancies to determine resultant changes in behavioral intentions. In this way, protection motivation theory was expanded to be made applicable to attitude-change attempts, and not just fear appeals alone (Maddux & Rogers, 1983). In their experiment on preventive health behavior (reduction or elimination of smoking), Maddux and Rogers (1983) found support for self-efficacy expectancy as a fourth component of protection motivation theory. Self-efficacy expectancy significantly influenced intentions to adopt the recommended coping behavior, and proved to be the most powerful predictor of behavioral intentions (Maddux & Rogers, 1983). Additionally, self-efficacy expectancy influenced the effect of probability of a threat's occurrence and coping response efficacy (Maddux & Rogers, 1983).

In the reformulated PMT, a differentiation was made between maladaptive threat appraisal and adaptive coping appraisal processes (Witte, 1992). In the threat appraisal process, people may continue to engage in maladaptive behaviors if the rewards of performing the maladaptive behavior are greater than the perceived severity of the danger and their perceived susceptibility to the danger (Witte, 1992). Furthermore, Prentice-Dunn and Rogers (1986) found that while an increase in the intrinsic rewards and extrinsic rewards will increase the probability of the maladaptive response, an increase in perceived threat (i.e., severity or susceptibility) will decrease the probability of the maladaptive response. Fear is considered to be another intervening variable, between perceptions of severity and vulnerability and the level of appraised threat (Norman, Boer,

& Seydel, 2005). If an individual perceives greater vulnerability to a serious threat, this will lead to greater fear, which will lead to a greater motivation to indulge in protective behavior (Norman, Boer, & Seydel, 2005). As for the coping appraisal, an increase in perceived response efficacy or self-efficacy will increase the likelihood of adaptive behavior, while an increase in response costs will decrease the likelihood of adaptive behavior (Witte, 1992). The schema of this revised reformulation of PMT is reproduced in Figure 2.2.

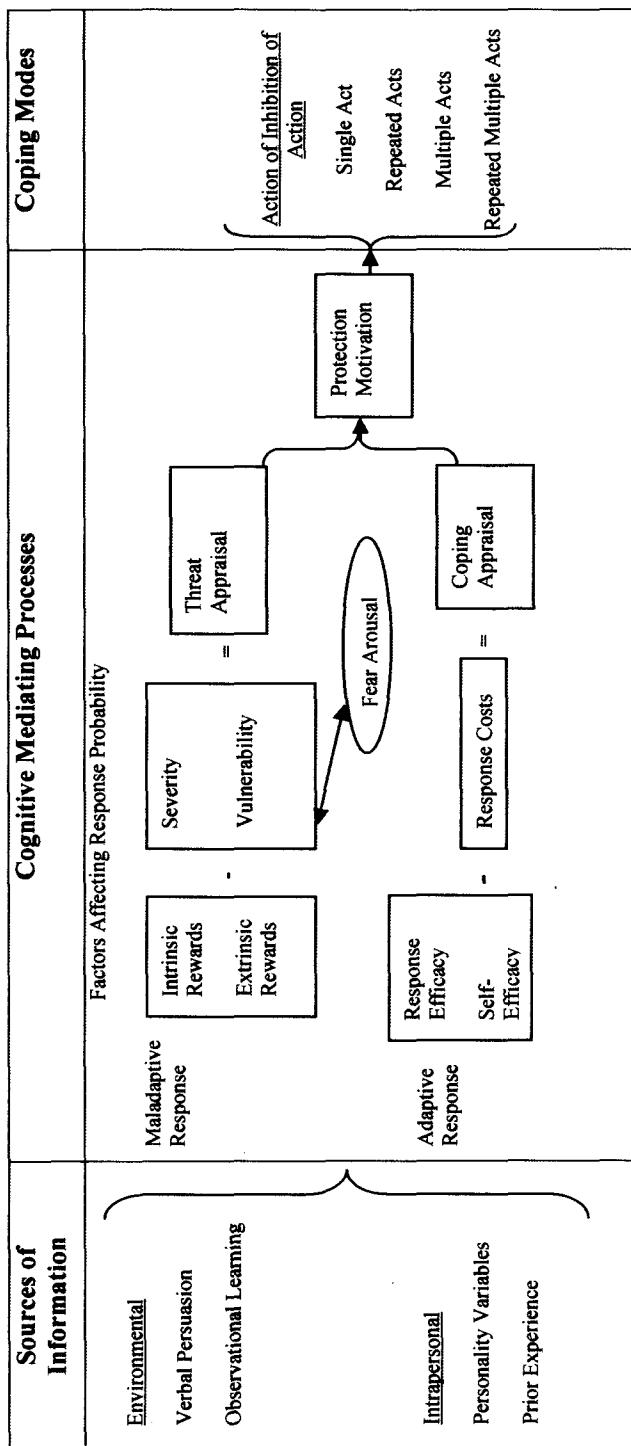


Figure 2.2. Schema of the Revised Protection Motivation Theory

Source: Witte (1992, p.335)

In summary, the motivation of the stakeholders to protect themselves from harm is enhanced by the following four perceptions: (1) the severity of the threat, (2) their vulnerability to the threat, (3) self-efficacy, i.e., their confidence in their ability to cope with the threat and perform threat reducing behaviors, and (4) response efficacy, i.e., the ability of the response to reduce the threat (Maddux & Rogers, 1983; Rogers, 1983). Protection motivation is operationalized in terms of intentions of 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). Rogers (1983) also found that various environmental (e.g., fear appeals) and intrapersonal (e.g., personality) sources of information can initiate two independent appraisal processes: threat appraisal and coping appraisal. 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, intrinsic and extrinsic rewards, 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).

Analysis of PMT

Two-way interactions between one of the threat variables and one of the efficacy variables have been consistently found in PMT studies, but specific interactions between the four variables have been difficult to predict (Witte, 1992).

As stated earlier, in the reformulated PMT, a differentiation was made between maladaptive threat appraisal and adaptive coping appraisal processes (Witte, 1992). In the threat appraisal process, people might continue to perform maladaptive behaviors as long as the rewards of performing such maladaptive behavior are greater than the perceived severity of the threat and their perceived susceptibility to the threat (Rogers, 1983; Witte, 1992). Therefore, while an increase in the intrinsic rewards and extrinsic rewards will increase the probability of the maladaptive response, an increase in perceived threat (i.e., severity or susceptibility) will decrease the probability of the maladaptive response (Rogers, 1986; Witte, 1992; Norman, Boer, & Seydel, 2005). As for the coping appraisal, an increase in perceived response efficacy or self-efficacy will increase the likelihood of adaptive behavior, while an increase in response costs will decrease the likelihood of adaptive behavior (Witte, 1992). Thus, an increase in perceptions of susceptibility/severity accompanied with few rewards should lead to a decrease in the likelihood of a maladaptive response, even when efficacy is held constant at a low level, provided that efficacy is greater than response costs (Witte, 1992, p.336).

But empirical research literature presents results that are contra-indicative of this derived prediction of the PMT model (Witte, 1992). Increased perceived threat will lead to an increase in maladaptive behaviors if perceived efficacy is low (Witte, 1992). When perceived efficacy is low, an increase in perceived threat will have no effect or else will

have a boomerang effect (Rogers 1983; Witte, 1992). Therefore, Witte (1992) concludes that from the revised graphic PMT model, one can neither derive nor explain the boomerang predictions.

The second flaw attributed to the PMT is that it does explain how threat appraisal and coping appraisal work in combination to result in protection motivation and therefore, subsequent behavior (Witte, 1992). When both threat and coping appraisals are high, they lead to decreases in maladaptive behaviors, and increases in adaptive behaviors, thus, leading to maximum protection motivation (Rogers 1983; Witte, 1992). But when coping appraisal is high (i.e., efficacy greater than costs), there should be an increase in adaptive behavior, and when threat appraisal is low (i.e., rewards greater than severity/susceptibility), there should be no change in maladaptive behaviors (Witte, 1992). This translates into an increase in adaptive behaviors (e.g., quit smoking cigarettes), while at the same time no change in maladaptive behaviors (e.g., continue smoking cigarettes); which is obviously logically inconsistent (Witte, 1992).

Therefore, it is concluded that the revised PMT model yields predictions that are inconsistent with empirical findings and does not explain the interaction between threat and coping appraisals and the resultant protection motivation and subsequent behaviors (Witte, 1992). The original PMT model with self-efficacy added to it, however, explains the factors leading to message acceptance (Witte, 1992). The original PMT model with self-efficacy added to it is depicted in Table 2.1.

Table 2.1. Schema of the Original Protection Motivation Theory with Self-Efficacy Added

Sources of Information	Processes	Outcomes
Probability of Occurrence	Perceived Susceptibility	Protection Motivation
Magnitude of Noxiousness	Perceived Severity	Intentions
Response Efficacy	Perceived Response Efficacy	Behaviors
Self-Efficacy	Perceived Self-Efficacy	

Source: Witte (1992, p.334)

Applications of PMT

PMT has been applied to studies on health promotion and disease prevention, injury prevention, political issues, environmental concerns, and protecting others (Floyd, Prentice-Dunn, & Rogers, 2000). The protection motivation concept includes any threat for which there is an effective recommended response (Floyd et al., 2000). Furthermore, Floyd et al. (2000) state that PMT components may be useful not only for individual, but also for community interventions.

In their meta-analysis, Floyd et al. (2000) found that 66% of the total included 65 studies fell into one of the six categories of subject matter that were studied: cancer prevention (11 studies, 17%), exercise/diet/healthy lifestyle (11 studies, 17%), smoking (6 studies, 9%), AIDS prevention (6 studies, 9%), alcohol consumption (5 studies, 8%), and adherence to medical-treatment regimens (4 studies, 6%). The rest of the studies covered the following subject areas (with only one or two studies falling under each category): prevention of nuclear war, environmental protection, wearing bicycle helmets, driving safely, child-abuse prevention, reducing caffeine consumption, seeking treatment for sexually transmitted diseases, inoculation against influenza, saving endangered species, improving dental hygiene, home radon testing, osteoporosis prevention,

marijuana use, seeking emergency help via 911, pain management during recovery after dental surgery, and safe use of pesticides (Floyd et al., 2000).

Application of PMT in Health Studies

PMT has a wide-spread application in the field of health studies. According to Beck and Frankel (1981), PMT is nothing, but a conceptualization of fearful health threat communications. According to PMT, people will be more likely to accept advice on protecting themselves from a health threat, when they are convinced of the seriousness of the threat, their susceptibility to it, and that the recommended actions will control or avoid the health threat (Beck & Frankel, 1981).

Floyd, Prentice-Dunn, and Rogers (2000) state that it is important to understand the psychological variables involved in the following of medical regimens because it is of value to not only the patients and their families, but also to the health-care services and physicians.

The meta-analysis conducted by Milne, Sheeran, and Orbell (2000) used stricter inclusion criteria and included only empirical applications of PMT to health-related intentions, concurrent behavior or future behavior. The results of the PMT meta-analyses indicate that stronger predictions of protection motivation and behavior are provided by the coping appraisal variables than the threat appraisal variables (Norman et al., 2005).

Impact of health threat warnings and fear appeals upon protective behavior

Beck and Frankel (1981) studied the impact of health threat warnings (or communications) upon protective behavior and consider perceived threat control to be comprised of response efficacy and personal efficacy (i.e., a person's perceived ability to perform the recommended action successfully). Empirical support was found for these

factors and personal efficacy was proved to be a more important determinant of protective health behavior than response efficacy (Beck & Frankel, 1981).

Maddux and Rogers (1983) conducted a factorial experiment amongst undergraduate college students to study the impact of fear appeals through anti-smoking messages on attitudinal change. The experiment was used to test a combined model of protection motivation theory and self-efficacy theory (Maddux & Rogers, 1983). The results provided support for self-efficacy as the fourth component of PMT (Maddux & Rogers, 1983). It was found that self-efficacy exerted a direct influence on intentions and interacted with two other variables of PMT.

Fear appeals

Fear appeals are a kind of communication involving a threat and have been studied in the field of marketing (Tanner, Jr., Day, & Crask, 1989). PMT recommends adding coping response information to fear appeals (Tanner, Jr., Day, & Crask, 1989). Tanner, Jr. et al. (1989) conducted a study to evaluate the impact of health threat communication in the form of marketing brochures on safe sex practices on a convenience sample of college students. The results of the study indicate that traditional threat-oriented fear appeals are less effective in comparison to appeals that also contain information about the coping response (Tanner, Jr. et al., 1989)

Tanner, Jr., Hunt, and Eppright (1991) re-conceptualized Rogers' (1983) PMT model into an ordered effects model called the Ordered Protection Motivation (OPM) model, which places "fear" in a key role in the threat and coping appraisal processes. The OPM model shows fear in both positive and negative roles, unlike the PMT (Eppright, Hunt, Tanner, Jr., & Franke, 2002). PMT offers a model to improve the effectiveness of

the fear appeal (Tanner, Jr., Hunt, & Eppright, 1991). Tanner, Jr. et al. (1991) proposed several changes to PMT and empirically tested their model in a study involving college students and their knowledge of sexually transmitted diseases (STDs) and how they responded to informative material of responsible sexual behavior. In the ordered PMT model, severity of threat and probability of occurrence are processed first along with the behavior appraisal, and this may evoke fear, which in turn leads to the processing of information on coping response and self-efficacy (Tanner, Jr. et al., 1991). Tanner, Jr. et al. (1991) advise marketers that in advertising it is not enough to present threatening information, but one must also change perceptions regarding the efficacy of maladaptive coping responses. Only then will the subjects be willing to consider alternative coping responses (Tanner, Jr. et al., 1991). Vulnerability beliefs or perceptions of personal risk may occupy a key role in the process of threat-persuasion (Eppright, Tanner, Jr., & Hunt (1994). Therefore, in their study Eppright et al. (1994) introduced two types of knowledge into the ordered protection motivation (OPM) model. Results from the study by Eppright et al. (1994) show that experimental AIDS prevention knowledge directly increased maladaptive or unsafe sex behaviors, while general AIDS problem knowledge led to an indirect increase in adaptive safe sex behaviors through certain OPM model mediators.

Eppright, Hunt, Tanner, Jr., and Franke (2002) evaluated the role of fear and maladaptive health behavior responses within the OPM threat persuasion framework in a study regarding testicular cancer. Eppright et al. (2002) recommend that in order to improve the coping appraisal process and increase adaptive protection behavior intentions, fear should act as an intervening variable between threat and coping appraisal.

In order to account for the inconsistencies found in earlier PMT research, Cismaru and Lavack (2007) propose that people should rank the PMT variables in terms of their perceived importance and should decide not to continue processing the information if the perceived level of any of the variables does not pass a minimum cut-off level. Cismaru and Lavack (2007) found that perceived cost is the main driver of persuasion. This study provides insight into the decision-making process of consumers with regard to recommended health behavior, and therefore, offers advice to marketing communicators and public health campaigners.

Impact of uncertainty orientation on protective behavior

According to Brouwers and Sorrentino (1993) the absence of higher order interactions between the components of Roger's (1983) PMT model could be partly attributed to uncertainty orientation. In an experiment involving college students, Brouwers and Sorrentino (1993) provided the subjects with threat information about Crevelling's disease. It was found that uncertainty-oriented subjects apparently followed predictions from PMT, and thus, showed a linear relation of compliance with an increase in threat and efficacy (Brouwers & Sorrentino, 1993). Those subjects, who were certainty-oriented, appeared not to follow the PMT model's predictions (Brouwers & Sorrentino, 1993).

In order to understand when to accentuate the negative in public service campaigns, Block and Keller (1995) conducted two experiments on the health related issues of sexually transmitted disease and skin cancer. Block and Keller (1995) showed that less certain conditions motivated more in-depth message processing. Further, it was found that negative frames are more persuasive than positive frames for in-depth

processing (Block & Keller, 1995). The results of their second study are consistent with PMT and indicate that the efficacy of the recommendations influences the intentions to cooperate (Block & Keller, 1995).

Determinants of non-compliance

In an application of PMT to sports injury rehabilitation, Taylor and May (1996) studied the determinants of non-compliance using PMT as a framework. Taylor and May (1996) found partial support for the role of threat and coping appraisals as determinants of compliance with sports injury rehabilitation. Enhancing the perception of threat and coping appraisal processes may lead to fewer non-compliant individuals (Taylor & May, 1996).

In order to find out how people coped with a threat when they did not plan to adopt any adaptive, protective response, Rippetoe and Rogers (1987) did a study on Breast cancer patients and found that the high-threat condition energized all forms of coping and it did not differentially cue specific coping strategies.

Extension of PMT related health studies to children and adolescents

Identifying a lack of published studies of PMT that presented health-threat communications to children, adolescents, and adults and thus, compared their responses, Sturges and Rogers (1996) applied PMT to children, adolescents, and adults in a study to evaluate the persuasiveness of health education messages pertaining to tobacco use. In children and adolescents, it was found that threat appeals worked only if they believed they could effectively cope with the danger.

PMT and subsequent behavior

PMT accounts well for intention to change, but it is limited in its ability to explain subsequent behavior (Floyd et al., 2000; Milne et al., 2000; Milne, Orbell, & Sheeran, 2002). Motivation is the starting point for behavioral performance (Milne et al., 2002). Adoption of a behavior has two distinct stages, namely, the motivational or deliberative phase, and the post-intentional or volitional phase (Gollwitzer, 1993; Heckhausen, 1991; Milne et al., 2002). In the motivational or deliberative phase, the individual weights the costs and benefits of performing a behavior and in the post-intentional or volitional phase, the individual strategizes and plans to ensure the enacting of his/her intentions (Milne et al., 2002). Thus, combining a motivational intervention based on PMT with a volitional intervention based on implementation intentions is more likely to increase exercise behavior than just a motivational intervention alone (Milne et al., 2002). It was found that motivational intervention increased threat and coping appraisal and intentions to engage in exercise significantly, but did not bring about any significant increase in subsequent exercise behavior (Milne et al., 2002). The combined protection motivation theory/implementation intention intervention showed dramatic effects on subsequent exercise behavior (Milne et al., 2002). The volitional intervention, however, influenced neither the behavioral intention nor any other motivational variables (Milne et al., 2002).

Inclusion of risk into PMT

Pechmann, Zhao, Goldberg, and Reibling (2003), applied PMT to identify effective message themes to convey anti-smoking advertisements for adolescents. Results show that those message themes that enhanced perceptions that smoking will lead to the risk of social disapproval, led to an increase in nonsmoking intentions amongst

adolescents (Pechmann et al. 2003). This finding lends support to the proposal by Ho (1998) to formally include social risks into PMT.

In a study to assess parents' perception of children's risk for recreational water illnesses (RWI), McClain, Bernhardt, and Beach (2005), developed a comprehensive scale using items based on constructs of PMT. The resulting perceived risk scale provides a way to measure the psycho-social factors that mediate or predict the adoption of behaviors that might prevent the spreading of infectious diseases contracted by children while swimming (McClain et al., 2005).

Application of PMT in Information Security Studies

Information security contravention behavior studies tend to focus on security lapses and behavior recommendations, but one of the crucial aspects of information security lies in understanding why people who know how to protect the information systems, fail to take the necessary protective measures (Workman, Bommer, & Straub, 2008). Therefore, in their empirical study, Workman et al. (2008), use PMT to test a threat-control model and understand the knowing-doing gap. A new variable, locus of control (i.e., perception that the threat is preventable) was introduced into their threat control model (TCM) (Workman et al., 2008). It was found that perceived severity of threat dictates the motivation to prevent the threat from happening and that self-efficacy and locus of control determine coping (Workman et al., 2008). Workman et al. (2008) highlight the counter-productivity of fear-appeals after a certain level.

Herath and Rao (2009) developed an Integrated Protection Motivation and Deterrence Model of security compliance. It was found that (a) while perceptions regarding severity of security breach, response efficacy and self-efficacy were likely to

have a positive effect on attitudes towards security policies, response cost negatively influences the favorable attitudes; (b) social influence significantly impacts compliance intentions; (c) resource availability is a significant factor enhancing self-efficacy; (d) self-efficacy is a significant predictor of policy compliance intentions; and (d) organizational commitment impacts intentions directly and promotes a belief that the actions of the employees have an effect on the over all information security of an organization (Herath & Rao, 2009).

Table 2.2 provides a listing and brief overview of some of the most noteworthy research contributing to not only theoretical advancement, but also application of PMT.

Table 2.2. PMT Research, Significance, Theoretical Advancement, and Contextual Application

Research	Significance	Theoretical Advancement	Contextual Application
Rogers (1975)	Fear appeals consists of (a) the magnitude of noxiousness of a depicted event, (b) the conditional probability that the event will occur provided that no adaptive behavior is performed or there is no modification of an existing behavioral disposition, and (c) the availability and effectiveness of a coping response that might reduce or eliminate the noxious stimulus.	Proposed protection motivation theory (PMT) to advance the understanding of fear appeals and attitude change	
Beck and Frankel (1981)	Personal efficacy was proved to be a more important determinant of protective health behavior than response		
Rogers (1983), Maddux & Rogers (1983)	Self-efficacy expectancy was included to PMT	Presented a more comprehensive model of PMT.	Studied the impact of fear appeals through anti-smoking messages on attitudinal change.

Table 2.2 (Continued)

Rippetoe and Rogers (1987)	Studied how people coped with a threat when they did not plan to adopt any adaptive, protective response and found that the high-threat condition energized all forms of coping and it did not differentially cue specific coping strategies.		Did a study on Breast cancer patients.
Tanner, Jr., Day, and Crask (1989)	Traditional threat-oriented fear appeals are less effective in comparison to appeals that also contain information about the coping response.		Evaluated the impact of health threat communication in the form of marketing brochures on safe sex practices on a convenience sample of college students.
Tanner, Jr., Hunt, and Eppright (1991)	Placed "fear" in a key role in the threat and coping appraisal processes. The OPM model shows fear in both positive and negative roles, unlike the PMT.	Re-conceptualized Rogers' (1983) PMT model into an ordered effects model called the Ordered Protection Motivation (OPM).	Empirically tested their model in a study involving college students and their knowledge of sexually transmitted diseases (STDs) and how they responded to informative material of responsible sexual behavior.
Brouwers and Sorrentino (1993)	Attributed the absence of higher order interactions between the components of Roger's (1983) PMT model partly to uncertainty orientation.		In an experiment involving college students, the subjects were provided with threat information about Creveling's disease.
Eppright, Tanner, Jr., and Hunt (1994)	Introduced two types of knowledge into the OPM model		Results from the study by Eppright et al. (1994) show that experimental AIDS prevention knowledge directly increased maladaptive or unsafe sex behaviors, while general AIDS problem knowledge led to an indirect increase in adaptive safe sex behaviors through certain OPM model mediators
Block and Keller (1995)	Efficacy of the recommendations influences the intentions to cooperate. Less certain conditions motivated more in-depth message processing. Negative frames are more persuasive than positive frames for in-depth processing.		Conducted two experiments on the health related issues of sexually transmitted disease and skin cancer.

Table 2.2 (Continued)

Sturges and Rogers (1996)	In children and adolescents, it was found that threat appeals worked only if they believed they could effectively cope with the danger.		Applied PMT to children, adolescents, and adults in a study to evaluate the persuasiveness of health education messages pertaining to tobacco use.
Taylor and May (1996)	Studied the determinants of non-compliance using PMT as a framework and found partial support for the role of threat and coping appraisals as determinants of compliance with sports injury rehabilitation.		Applied PMT to sports injury rehabilitation.
Eppright, Hunt, Tanner, Jr., and Franke (2002)	In order to improve the coping appraisal process and increase adaptive protection behavior intentions, fear should act as an intervening variable between threat and coping appraisal.		Evaluated the role of fear and maladaptive health behavior responses within the OPM threat persuasion framework in a study regarding testicular cancer.
Milne, Orbell, and Sheeran (2002)	PMT explains intention to change, but does not explain subsequent behavior, but combining a motivational intervention based on PMT with a volitional intervention based on implementation intentions, is more likely to increase exercise behavior than just a motivational intervention alone.		A longitudinal study conducted undergraduate students to study the impact of a combined motivational and volitional intervention on exercise behavior.
Pechmann, Zhao, Goldberg, and Reibling (2003)	Found support to formally include social risks into PMT. Message themes that enhanced perceptions that smoking will lead to the risk of social disapproval, led to an increase in nonsmoking intentions amongst adolescents		Studied the impact of message themes to convey anti-smoking advertisements for adolescents in order to determine the most effective themes.
McClain, Bernhardt, and Beach (2005)	Developed a comprehensive scale using items based on constructs of PMT. The resulting perceived risk scale provides a way to measure the psycho-social factors that mediate or predict the adoption of behaviors that might prevent the spreading of infectious diseases contracted by children while swimming.		Conducted a study to assess parents' perception of children's risk for recreational water illnesses (RWI).

Table 2.2 (Continued)

Cismaru and Lavack (2007)	Found that perceived cost is the main driver of persuasion.	Proposed that people should rank the PMT variables in terms of their perceived importance and should decide not to continue processing the information if the perceived level of any of the variables does not pass a minimum cut-off level.	
Workman, Bommer, and Straub (2008)	Used PMT to test a threat-control model and understand the knowing-doing gap.	A new variable, locus of control (i.e., perception that the threat is preventable) was introduced into their threat control model (TCM)	A field study was conducted amongst people from a large technology-oriented services corporation to understand the knowing-doing gap.
Herath and Rao (2009)	(a) Response cost negatively influences the favorable attitudes; (b) social influence significantly impacts compliance intentions; (c) resource availability is a significant factor enhancing self-efficacy; (d) self-efficacy is a significant predictor of policy compliance intentions; and (d) organizational commitment impacts intentions directly and promotes a belief that the actions of the employees have an effect on the over all information security of an organization	Developed an Integrated Protection Motivation and Deterrence Model of security compliance	Empirically test the theoretical model with a data set representing the survey responses of 312 employees from 78 organizations.

Model Development and Hypotheses

In today's world, every organization is an open-system, and as such these organizations have no choice, but to interact with the environment (Adam & Haslam, 2001). This interaction, in its wake brings about uncertainty, and the threat of disaster is one such uncertainty (Adam & Haslam, 2001). In the area of information systems, one way in which organizations plan and prepare for disasters is by preparing the IS disaster recovery plans (Adam & Haslam, 2001).

As stated earlier, a Faulkner Information Services research study found that 50% of companies that suffer from data loss due to disasters go out of business within 24 months (Chisholm, 2008). This highlights the importance of disaster recovery planning. Yet, according to Bolch (2008), between 2003-2004, more than 70% of companies had participated in mock DR drills, but now the number has dropped down to 20%-30%. Not only that, but Bolch (2008) states that the mood of the business community towards DR is apathetic. This statement resonates with the opinion of Farazmand (2007), who pointed out that despite the losses due to Hurricane Katrina; many firms are still very negligent about DRP. Moreover, according to the Info-Tech Research Group report, 60% of North American businesses do not have a DR plan (Chisholm, 2008).

From all this, it is evident that despite the mission critical importance of disaster recovery planning, many organizations fail to have adequate or no disaster recovery plans. This leads to the question of “why are firms still negligent about DRP?” This question is the driving force behind this research study.

In order to study the reason behind this negligence towards disaster recovery planning, theoretical frameworks were explored. According to Whetten (1989), a theory provides answers to questions of what, how, why, who, where, and when. Herzog (2007) specifically believes that theory and planning are related. Planning is nothing, but preparation to reduce the effects of any future event, and theories aid the planners to achieve this goal; therefore, theories can serve as a foundation for planning (Herzog, 2007). Further, planning is considered to be the bridge or connection between theory and action (Herzog, 2007). Therefore, it can be concluded that there has to be a possible

explanation in theory to the research question of why don't organizations undertake DRP, despite knowing the critical significance of it.

Although, DRP has been studied through many theoretical applications, there still does not seem to be an explanation grounded in theory for this confounding question of why don't organizations undertake DRP, despite knowing the critical significance of it.

It is evident from a review of the literature that PMT has been applied in various fields to study the motivation behind protection behaviors. Apart from its application in various health related fields, PMT has also found application in information security studies. As noted earlier in the literature review on PMT, Workman et al. 2008, applied PMT to study why people who know how to protect the information systems, fail to take the necessary protective measures. In their empirical study, Workman et al. (2008), use PMT to test a threat-control model and understand the knowing-doing gap. Therefore, in light of all this, PMT seems to be an appropriate lens through which to study DRP and discover answers to the compelling question of why DRP is not undertaken seriously. In this study an effort is made to study disaster recovery planning through the lens of PMT to explain what could be the factors influencing disaster recovery planning in organizations. This is demonstrated in the conceptual model presented in Figure 2.3.

DRP will be the dependent variable in the conceptual model of this study. Since this will be an empirical study, there is a need to measure DRP. But as stated earlier, although, a galore of literature is published on the semantic differences between DRP and business continuity planning, the measurement of DRP has not received much attention until recently.

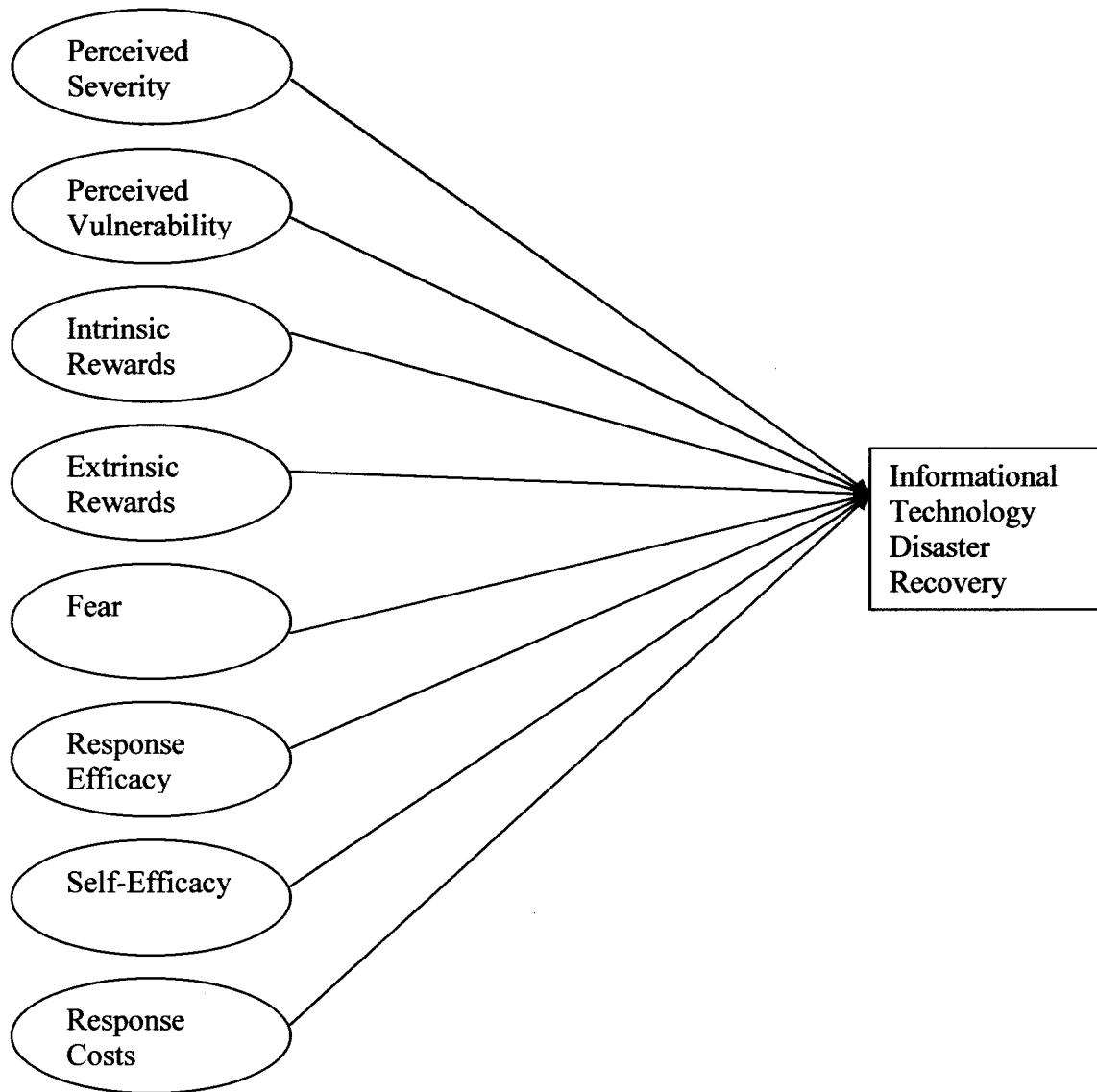


Figure 2.3. Original Conceptual Research Model

Shropshire and Kadlec (2009) has provided a domain definition of information technology disaster recovery planning (ITDRP) covering seven dimensions, leading to the development of a 34 item measure for assessing the degree of ITDRP. Therefore, for the purpose of this study, ITDRP will be considered to be the main outcome/dependent variable.

As stated earlier, DRP although discussed in text books, has not received attention in mainstream IS research, which boasts of only 6 articles that were published in peer-reviewed MIS journals in the past ten years (Shropshire & Kadlec, 2009). Therefore, it is believed that this research study will make a value-added contribution to IS research by exploring the factors influencing DRP in organizations.

Outcomes of the Model

As stated earlier, in the reformulated PMT, a differentiation was made between maladaptive threat appraisal and adaptive coping appraisal processes (Witte, 1992). For instance, the maladaptive behavior could be to continue smoking cigarettes and the adaptive behavior could be to quit smoking cigarettes. In the context of the current study on disaster recovery planning, the adaptive behavior is assumed to be greater ITDRP, and the maladaptive behavior is assumed to be lower ITDRP. It is evident here, that PMT is being adapted to suit the context of the current study.

It has been stated earlier that in the threat appraisal process, people may continue to engage in maladaptive behaviors if the rewards of performing the maladaptive behaviors are greater than the perceived severity of the danger and their perceived susceptibility to the danger (Witte, 1992). In other words, greater perceived severity and vulnerability to threat should lead to an increase in the adaptive behavior (i.e., ITDRP here). Also greater intrinsic and extrinsic rewards for the maladaptive behavior, should lead to a decrease in the adaptive behavior (i.e., ITDRP here). This leads to the following hypotheses.

H1: Perceived severity will have a significant positive effect on an organization's information technology disaster recovery planning (ITDRP).

H2: *Perceived vulnerability will have a significant positive effect on an organization's information technology disaster recovery planning (ITDRP).*

H3: *Intrinsic rewards will have a significant negative effect on an organization's information technology disaster recovery planning (ITDRP).*

H4: *Extrinsic rewards will have a significant negative effect on an organization's information technology disaster recovery planning (ITDRP).*

If an individual perceives greater vulnerability to a serious threat, this will lead to greater fear, which will lead to a greater motivation to indulge in protective behavior (Norman, Boer, & Seydel, 2005). Therefore, it is hypothesized that greater fear will lead to greater ITDRP. This is presented in the form of hypothesis as follows.

H5: *Fear will have a significant positive effect on an organization's information technology disaster recovery planning (ITDRP).*

A high coping appraisal (i.e., greater efficacy over costs), will lead to an increase in adaptive behaviors (Witte, 1992). In other words, greater response efficacy and self-efficacy should lead to an increase in adaptive behavior (i.e., ITDRP here); while greater response costs should lead to a decrease in the adaptive behavior (i.e., ITDRP here). Therefore, the following hypotheses are presented. Table 2.3 lists all the hypotheses presented in this chapter.

H6: *Response efficacy will have a significant positive effect on an organization's information technology disaster recovery planning (ITDRP).*

H7: *Self-efficacy will have a significant positive effect on an organization's information technology disaster recovery planning (ITDRP).*

H8: Response costs will have a significant negative effect on an organization's information technology disaster recovery planning (ITDRP).

Table 2.3. Hypotheses

H1: Perceived severity will have a significant positive effect on an organization's information technology disaster recovery planning (ITDRP).
H2: Perceived vulnerability will have a significant positive effect on an organization's information technology disaster recovery planning (ITDRP).
H3: Intrinsic rewards will have a significant negative effect on an organization's information technology disaster recovery planning (ITDRP).
H4: Extrinsic rewards will have a significant negative effect on an organization's information technology disaster recovery planning (ITDRP).
H5: Fear will have a significant positive effect on an organization's information technology disaster recovery planning (ITDRP).
H6: Response efficacy will have a significant positive effect on an organization's information technology disaster recovery planning (ITDRP).
H7: Self-efficacy will have a significant positive effect on an organization's information technology disaster recovery planning (ITDRP).
H8: Response costs will have a significant negative effect on an organization's information technology disaster recovery planning (ITDRP).

CHAPTER 3

RESEARCH METHODS

In this chapter, firstly, an overview of the variables used in the study will be presented along with their descriptions. This will be followed by a description of the data collection survey instrument that was developed based on various existing valid and reliable scales that were adapted for the purpose of this study. Lastly, the statistical methodology expected to be used to analyze the data will be briefly stated.

Variables

Each of the variables used in the conceptual model will be defined in the following sub-sections.

PMT Constructs

The protection motivation theory identifies eight constructs, which are presented in Table 3.1. 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, intrinsic and extrinsic rewards, and fear arousal (Maddux & Rogers, 1983; Rogers, 1983; Milne, Orbell, & Sheeran, 2002). Fear is considered to be another intervening variable, between perceptions of severity and vulnerability and the level of appraised threat (Norman, Boer, & Seydel, 2005). The variables used in coping appraisal are beliefs about

response efficacy (i.e., the ability of the response to reduce the threat), self-efficacy (i.e., their confidence in their ability to cope with the threat and perform threat reducing behaviors), and response costs (Maddux & Rogers, 1983; Rogers, 1983; Milne, Orbell, & Sheeran, 2002). All these constructs and their definitions are presented in Table 3.1.

Table 3.1. PMT Variables

PMT Variable	Definition
Severity of the threat	Perceived severity of a threatened event.
Vulnerability to the threat	Perceived probability of occurrence of a threatened event.
Intrinsic Rewards	Rewards that a person experiences from within for actually doing the maladaptive behavior (e.g., pleasure).
Extrinsic Rewards	Rewards that a person experiences from the external/outside world for doing maladaptive behavior (e.g., social approval).
Fear	If the available coping responses are inadequate, then fear is aroused.
Response efficacy	Efficacy of the recommended preventive behavior.
Self-efficacy	Self-confidence or belief in one's own ability to perform the recommended preventive behavior.
Response costs	Costs associated with the response/recommended preventive behavior.

Determinants of ITDRP

Shropshire and Kadlec (2009) has provided a domain definition of information technology disaster recovery planning (ITDRP) covering seven dimensions, leading to the development of a 34 item measure for assessing the degree of ITDRP. According to the systematically-developed definition of Shropshire and Kadlec (2009), IT disaster recovery planning comprises of the seven dimensions: IT disaster identification and notification, preparing organizational members, IT services analysis, recovery process, backup procedures, offsite storage, and maintenance. These seven dimensions represent

the collective actions that firms need to take in order to ensure recovery post IT disasters (Shropshire & Kadlec, 2009). Based on Shropshire and Kadlec (2009) these seven dimensions of ITDRP are listed and defined in Table 3.2.

Table 3.2. ITDRP Dimensions

ITDRP Dimension	Description
IT Disaster Identification & Notification Procedures <ul style="list-style-type: none"> - Detection - Warning - Means of Warning 	<p>It is based on procedures developed for detecting IT disasters, communicating during emergencies, and for warning IT disaster recovery team members and other stakeholders.</p> <ul style="list-style-type: none"> - Detection: Based on identification of IT disasters and includes procedures for distinguishing between a loss of service inputs and a loss of IT services. - Warning: Includes actions taken to warn IT disaster recovery team members when a crisis occurs. - Means of Warning: Represents the establishment of communication channels to be used during the disaster.
Preparing Organizational Members <ul style="list-style-type: none"> - ITDR Team Prep - Non-Team Prep - Decision Making 	<p>Includes procedures for IT disaster recovery team training, briefing for key non-team members, and the formalization of a decision-making structure.</p> <ul style="list-style-type: none"> - ITDR Team Prep concerns the organization ITDR team. - Addresses the training and briefing of non-team members in the event of a disaster. - Addresses procedures for decision making authority under a variety of circumstances.
IT Services Analysis <ul style="list-style-type: none"> - IT Services - Risks to Services - Prioritizing IT Services 	<p>Includes three sub-domains for cataloging IT services, prioritizing IT services in terms of reactivation, and identifying potential threats.</p> <ul style="list-style-type: none"> - IT services identification involves an exhaustive review of all the services the IT department offers to the other departments within an organization. - Focus is on identification of risks to IT services and associated infrastructures. - Involves procedures for ranking IT services in the order in which they need to be restored.
Recovery Process <ul style="list-style-type: none"> - Alternative Facilities - Recovery Procedures 	<p>Includes procedures for restoring IT service inputs and for switching IT operations to alternative facilities.</p> <ul style="list-style-type: none"> - Involves procurement of alternative facilities for hosting IT operations in the event of the primary site going offline. - Process of restoring basic IT service inputs
Backup Procedures	<p>Based on routines developed for creating backup copies of data, software, configuration files, and IT disaster recovery plan.</p>
Offsite Storage <ul style="list-style-type: none"> - Portability - Offsite Locations to Backup 	<p>Includes procedures for ensuring that systems, software and data are made as portable as possible, and that offsite locations have been selected for use as backup storage sites.</p> <ul style="list-style-type: none"> - Organizing data, software, and other documents into formats which are easy to transport. - Procedures for transporting and storing data, software, configuration files, and copies of the IT disaster recovery plan at alternative locations.

Table 3.2 (Continued)

Maintenance	<ul style="list-style-type: none"> - Testing and updating - Documentation - Synchronizing 	<p>Plans for testing and updating the ITDRP and its associated documentation for ensuring that the ITDRP fits within the scope of the business continuity plan.</p> <ul style="list-style-type: none"> - Includes procedures for continually testing and updating an ITDRP. - Updating documentation such as configuration manuals, network schematics, and change logs on a regular basis. - Ensures that the ITDRP falls in line with the business continuity plan.
--------------------	--	--

Instrument Design

All the constructs used in this study, except for intrinsic and extrinsic rewards, were measured using well validated multi-item scales drawn from the literature of PMT and disaster recovery. The themes on intrinsic and extrinsic rewards identified by Posey (2010) were used as a foundation to further develop the intrinsic and extrinsic rewards items for this study. Four subject matter experts (two professors of information systems and two doctoral students of information systems) performed the content validity assessment. All the scales used in this study are listed in Table 3.3. The actual survey instrument used in this study is presented as Appendix A.

Table 3.3. Scales

Construct	Scale
Severity of Threat	Witte, Cameron, McKeon, & Berkowitz (1996); Milne, Orbell, & Sheeran (2002)
Vulnerability to Threat	Milne, Orbell, & Sheeran (2002); McClain, Bernhardt, & Beach (2005); Witte, Cameron, McKeon, & Berkowitz (1996)
Intrinsic Rewards	Developed for this study based on themes identified by Posey (2010)
Extrinsic Rewards	Developed for this study based on themes identified by Posey (2010)
Response Efficacy	Milne, Orbell, and Sheeran (2002) Witte, Cameron, McKeon, & Berkowitz (1996)
Self-Efficacy	Milne, Orbell, and Sheeran (2002) Witte, Cameron, McKeon, & Berkowitz (1996)

Table 3.3 (Continued)

Response Costs	Milne, Orbell, and Sheeran (2002)
Fear	Milne, Orbell, and Sheeran (2002); Eppright, Hunt, Tanner, Jr., Franke (2002); Block and Keller (1995)
Information Technology Disaster Recovery Planning (ITDRP)	Shropshire and Kadlec (2009)

Scale Computation

Following Petter, Straub, and Rai (2007) it is determined that the conceptual model in *Figure 2.3* has both reflective and formative constructs. For reflective constructs, the direction of causality is from the constructs to the indicators; indicators for each construct are interchangeable and dropping an indicator does not alter the conceptual domain of the constructs; the indicators for each construct are expected to covary with each other; and indicators for each construct had the same antecedents and consequences (Petter et al. 2007). The rules to identify formative construct are just the opposite of those stated for reflective constructs. Following these rules, it was assessed that the research model in this study consists of both formative and reflective constructs.

Reflective measures are also called effect indicators or reflectors (Pedhazur & Schmelkin, 1991). They reflect the effect of the latent variables (Pedhazur & Schmelkin, 1991; Diamantopoulos & Winklhofer, 2001). Formative measures are also called as cause indicators (Pedhazur & Schmelkin, 1991; Diamantopoulos & Winklhofer, 2001). They are the cause of the latent variables (Pedhazur & Schmelkin, 1991; Diamantopoulos & Winklhofer, 2001). The research model for this study consists of both formative and reflective constructs.

Based on the guidelines by Petter, Straub, and Rai (2007), the constructs identified as either formative or reflective in the model are all listed in Table 3.4. Over all scales or indexes were computed based on whether the constructs were reflective or formative in nature. If they were reflective, by following Gefen, Straub, and Boudreau (2000), the over all scale or index was computed by taking an average of all the individual items making up the scale. If the constructs were formative, by following Bagozzi (1994) and Diamantopoulos and Winklhofer (2001), the over all scale or index was computed by doing a summation of all the individual items that make up the scale.

Table 3.4. Nature of Constructs and Scale Computation

Construct	Formative/Reflective	Scale Computation
Perceived Severity	Reflective	Average
Perceived Vulnerability	Reflective	Average
Intrinsic Rewards	Formative	Summation
Extrinsic Rewards	Formative	Summation
Fear	Reflective	Average
Response Efficacy	Reflective	Average
Self-Efficacy	Reflective	Average
Response Costs	Reflective	Average
Identification and Notification Procedures	Formative	Summation
Preparing Organizational Members	Formative	Summation
IT Service Analysis	Formative	Summation
Response Process	Formative	Summation
Back-up Procedures	Formative	Summation
Offsite Storage	Formative	Summation
Maintenance	Formative	Summation

Construct Validity and Reliability

If instruments are not valid, then it will result in misleading results and distortion of knowledge (Straub, 1989). In order to remedy the concerns regarding the poor validation efforts in the IS field, Straub (1989) demonstrated an instrument validation exercise that provides very valuable step-by-step insights into the process of validation. Straub (1989) strongly cautions, adapting existing scales by changing the format, and words, etc., would raise a question regarding the validity of the derived instrument. Therefore, it is imperative to ensure the validity of any instrument used in research. As suggested by Straub (1989), a principal components factor analysis is done to ensure construct validity.

The accuracy with which an instrument measures, such that it measures in the same way every time under the same conditions and with the same subjects, is called reliability (Kerlinger & Lee, 2000). Internal consistency, a method by which reliability can be estimated, is based on the idea that items or subparts of an instrument measure the same phenomenon (Pedhazur & Schmelkin, 1991). Coefficient alpha or Cronbach's alpha, which is a summary measure of the intercorrelations that exists amongst a set of items, is a popular estimate of internal consistency-reliability (Pedhazur & Schmelkin, 1991; Churchill, Jr.& Iacobucci, 2002). It is recommended that no matter which measure of internal consistency is used, an internal consistency reliability of .70 in the early stages of research, and a value above .80 or .90 in the advanced stages of research is considered satisfactory, while anything below .60 would indicate a lack of reliability (Nunnally & Bernstein, 1994).

According to Diamantopoulos and Winklhofer (2001), the validity and reliability techniques used for scales composed of reflective indicators are not appropriate for composite indexes with formative indicators. In the context of indexes based on formative indicators, Diamantopoulos and Winklhofer (2001) state that content specification, indicator specification, indicator collinearity, and external validity are critical. The content specification (i.e., specification of the scope of the latent variable) and indicator specification (i.e., items used as indicators cover the entire scope of the latent variable as described in the content specification) criteria described by Diamantopoulos and Winklhofer (2001) were followed during the scale development process. According to Diamantopoulos and Winklhofer (2001), multicollinearity amongst indicators makes it difficult to separate the distinctive influence of each of the indicators on the latent variables. Therefore, statistical tests were conducted to rule out multicollinearity. A variance inflation factor (VIF) $> 3.3 - 4$ is considered as an indication of multicollinearity (Petter et al, 2007; Diamantopoulos et al, 2008).

Discussing external validity, Diamantopoulos and Winklhofer (2001) caution against elimination of indicators as it may change the construct itself from a theoretical perspective. Petter et al. (2007) suggest using principal components analysis for assessing the construct validity of formative constructs. Therefore, a principal components analysis (PCA) was performed to asses the construct validity of the formative constructs.

Data Collection

Disaster recovery planning being a sensitive topic for many organizations, it was difficult to gain access to individuals in organizations to take the survey. Therefore, the data for this study was collected using Zoomerang, an external panel provider. The panel

consisted of individuals who were involved in the DRP process. The respondents were guaranteed anonymity. The survey questionnaire included not only the items that operationalized the constructs in the research model, but also included questions on demographics, experience of the respondents in DRP, etc.

A reliability check question was placed in the survey asking respondents to leave that particular item blank. This was done to identify responses by individuals who did not pay adequate attention while answering the survey. By doing this, it was assured that the remaining responses were reliable. The profile of the respondents is given in Table 3.5.

Table 3.5. Respondent Profile

	Count	Percentage
Gender		
Female	60	32.61%
Male	124	67.39%
Age		
Less than 21 yrs		
21-25 yrs		
26-35 yrs	20	10.87%
36-45 yrs	47	25.54%
46-55 yrs	64	34.78%
Over 55 yrs	53	28.80%
Education		
High School	25	13.59%
Bachelor's	102	55.43%
Master's	45	24.46%
Professional	7	3.80%
Doctorate	5	2.72%
Organizational Size		
1-100	60	32.61%
101-500	20	10.87%
501-1,000	23	12.50%
1,001-5,000	34	18.48%
More than 5,000	47	25.54%

Table 3.5 (Continued)

Experience in Current Organization		
Less than 1 yr		
1-5 yrs	10	5.43%
6-10 yrs	35	19.02%
11-15 yrs	49	26.63%
16-20 yrs	36	19.57%
21 yrs or more	20	10.87%
	34	18.48%
Experience in DRP in Current Organization		
Less than 1 yr		
1-5 yrs	29	15.76%
6-10 yrs	56	30.43%
11-15 yrs	60	32.61%
16-20 yrs	17	9.24%
21 yrs or more	7	3.80%
	15	8.15%
Job Profile		
Information Technology	149	80.98%
Other	35	19.02%
Industry of Organization		
Manufacturing	25	13.59%
Retail	5	2.72%
Services	67	36.41%
Entertainment	4	2.17%
Education	15	8.15%
Voluntary not for profit	3	1.63%
Other	65	35.33%
Company is Organized as:		
Publicly Traded Corporation	47	25.54%
Privately Held Corporation	68	36.96%
Non-Profit Corporation	23	12.50%
Limited Liability Company (LLC)	17	9.24%
Partnership	5	2.72%
Other	24	13.04%
Annual Revenue		
Less than \$1 million	49	26.63%
\$1 million-\$10 million	25	13.59%
\$11 million-\$100 million	43	23.37%
\$101 million-\$1 billion	25	13.59%
More than \$1 billion	42	22.83%

Statistical Methodology

Although in the initial stages of the study, before the data was collected, Partial Least Squares (PLS) was considered as a possible statistical technique that could be used as it is recommended by Chin (2000) for studies where the sample size is small and the research model has both formative and reflective constructs. But after data collection

with a resulting sample size of only 184, following Gefen, Straub, and Boudreau (2000), it seemed more appropriate to use the statistical technique of linear regression for the data analysis. For the required minimum sample size for PLS, Gefen, Straub, and Boudreau (2000) suggest the heuristic of having “at least 10 times the number of items in the most complex construct” (pg. 9). Considering the complexity of the model and the available sample size being only 184, it seemed more appropriate to use linear regression as it supports smaller sample sizes. Therefore, for the purpose of this study, the data was analyzed using multiple linear regression.

CHAPTER 4

DATA ANALYSIS AND RESULTS

The purpose of this chapter is to present the results of the tests conducted in order to analyze the data and investigate the research model. First, the results from the validity and reliability assessment of the survey instrument are presented. Next, the results of the regression analysis are presented.

Validity and Reliability Assessment

As suggested by Straub (1989), a principal components factor analysis was done to ensure construct validity. Petter et al. (2007) suggest using principal components analysis for assessing the construct validity of formative constructs. Therefore, a principal components analysis (PCA) was performed to assess the construct validity of the formative constructs. Principal components method was used for extraction and varimax for rotation. Hair et al. (1998) recommended that there should be no cross loadings of items above .40 and it was recommended by Churchill (1979) that items not loading properly may be dropped from the instrument. Examining the items in light of these recommendations some items were omitted from the model. Perceived severity and perceived vulnerability were loading on the same factor and based on closer examination

of the items it was found that there was some conceptual overlap between the items of both these constructs. Therefore, it was thought more advisable to drop perceived severity completely from the model and retain the items for perceived vulnerability. The results are presented in Table 4.1 for the reflective PMT constructs, in Table 4.2 for the formative PMT constructs, and in Table 4.3 for the formative ITDRP dependent variable constructs. Based on a closer examination of the individual items and the loadings, two of the ITDRP constructs, namely, preparing organizational members and IT service analysis were removed from the model. Iterations of PCA on the sub-dimensions of the over all ITDRP construct revealed that several items belonging to different sub-dimensions were factoring together. A re-examination of these items revealed that there was some conceptual overlap and that the situation warranted a regrouping of these items into three new separate constructs, namely: (1) identification, recovery, and back-up procedures; (2) procedures for the DRP plan, human resources, and physical facilities; and (3) offsite storage. The results from this iteration of the PCA analysis are presented in Table 4.3.

Table 4.1. Loadings for PMT Reflective Constructs

Items	Fear	Response Efficacy	Self-Efficacy	Perceived Vulnerability	Response Costs
REVPV1: We are unlikely to face any disaster in the future.	0.09223	-0.02495	-0.0396	.714	-.397
PV5: Our organization is at risk from a disaster.	.336	0.06213	0.03254	.700	.178
PV6: It is likely that our organization will be impacted by a disaster.	.169	0.05569	-0.01542	.825	0.06976
F1: I am frightened by the thought of our organization facing a disaster.	.832	0.06094	-.101	0.05723	0.05088
F2: My perception of the threat of disaster to our organization makes me feel tense.	.881	-0.05021	-0.03294	.220	-0.04835

Table 4.1 (Continued)

F3: My perception of the threat of disaster to our organization makes me feel uncomfortable.	.896	0.01792	-0.07047	.123	0.04268
F4: I feel fearful as I hear about threats to our organization due to a disaster.	.860	-0.04919	0.01765	.119	0.05291
F5: I feel nervous as I hear about threats to our organization due to a disaster.	.885	0.01258	-0.001365	.152	.102
RE1: Disaster recovery planning is a good way of reducing the risk of suffering systems and information loss due to a disaster.	0.01018	.855	0.08452	0.06854	-.330
RE2: If we were to implement the recommendations of disaster recovery planning, then the company would lessen the chances of suffering systems and information loss due to a disaster.	0.003036	.883	0.0233	-0.05064	-0.008226
RE4: Disaster recovery planning is an effective method to prevent loss and damage to information systems due to a disaster.	-0.005203	.820	.135	.100	-.244
SE2: I feel confident in my ability to implement the disaster recovery planning recommendations.	-0.03541	.272	.754	.107	-0.08997
SE4: To implement the disaster recovery planning recommendations would be easy for me.	-0.07555	0.003027	.902	-0.09035	-0.0301
SE6: Implementing disaster recovery planning is easy to do in order to prevent the loss and damage due to disaster.	-0.02692	-0.01072	.846	-0.0249	-0.07197
RC2: Implementing the disaster recovery planning recommendations would cause us too many problems.	0.00702	-.418	-0.05089	0.01155	.819
RC3: We would be discouraged from implementing the disaster recovery planning recommendations because it would take too much time.	.173	-.192	-.159	-0.001108	.864

Table 4.2. Loadings for PMT Formative Constructs

Items	Intrinsic Rewards	Extrinsic Rewards
IR1: I feel fine without a disaster recovery plan in the organization.	.816	.331
IR3: Not having a disaster recovery plan does not affect my morale negatively.	.849	.216
IR4: Not having a disaster recovery plan in the organization does not indicate that we are not prepared and it does not increase my worry.	.845	.271
IR5: Not having a disaster recovery plan indicates that the organization is focused on the day to day operations and that makes me feel secure.	.745	.317
ER1: Disaster recovery planning is expensive, so not undertaking disaster recovery planning will save money.	.237	.863
ER2: Disaster recovery planning ties up resources, so not implementing disaster recovery planning will make resources available for productive uses.	.276	.875
ER3: Not implementing disaster recovery planning will save a lot of time.	.384	.800

Table 4.3. Loadings for ITDRP Constructs

Items	Identification, Recovery, and Back-Up Procedures	Procedures for the DRP Plan, Human Resources, and Physical Facilities	Offsite Storage
INP2: We have a means of assessing the magnitude of information technology disasters.	.715	.366	.304
INP3: We have procedures for alerting individuals responsible for information technology disaster recovery.	.694	.260	.472
INP4: We have procedures for letting stakeholders know that an information technology disaster has occurred	.629	.098	.502
INP5: We have established an alternative means of communications (e.g. cell phones) to use in emergencies.	.718	.323	.296
RP6: We have procedures for recovering servers.	.767	.398	.213

Table 4.3 (Continued)

RP7: We have procedures for recovering applications and software.	.757	.389	.216
RP8: We have procedures for recovering data.	.741	.376	.244
BP1: We have procedures for creating backup copies of data.	.711	.243	.090
BP2: We have procedures for creating backup copies of software.	.741	.323	.102
BP3: We have procedures for creating backup copies of configuration files, change logs, and other documents.	.738	.343	.106
RP3: Our plans account for possible losses of human resources (i.e. missing or injured information technology workers).	.353	.645	.334
RP4: We have procedures for restoring physical facilities such as physical buildings, power, and cooling systems.	.370	.686	.301
BP4: We have procedures for creating backup copies of the disaster recovery plan itself.	.430	.753	.209
MAINT1: We have procedures for testing of the information technology disaster recovery plan.	.323	.832	.264
MAINT2: We have procedures for updating the information technology disaster recovery plan.	.444	.765	.334
MAINT3: We have procedures for ensuring that the information technology disaster recovery plan is part of the business continuity plan.	.388	.813	.329
OSS2: We have offsite locations for storing data.	.193	.277	.834
OSS3: We have offsite locations for storing software.	.220	.370	.819
OSS4: We have offsite locations for storing configuration files, change logs, and other relevant documents.	.208	.292	.873

The items pertaining to identification, recovery, and back-up procedures all deal with procedures related with dealing with the disaster and recovering from it and ensuring back-ups. The second construct deals primarily with procedures for activities such as procedures for taking care of the disaster plan itself, human resources, and the physical facilities. The third new construct is about offsite storage locations.

As stated earlier, it is not only important to check the validity of scales, but also the reliability. A reliability analysis was performed on the resulting revised scales after the validation process. The Cronbach's alphas resulting from the reliability analyses for the independent variables are presented in Table 4.5 and that for the dependent variables are presented in Table 4.4.

Table 4.4. Reliability Analysis for Independent Variables

Scale	Cronbach's Alpha
Perceived Vulnerability	.6706
Intrinsic Rewards	.8854
Extrinsic Rewards	.8798
Fear	.9295
Response Efficacy	.8538
Self-Efficacy	.7974
Response Costs	.8411

Table 4.5. Reliability Analysis for Dependent Variables

Scale	Cronbach's Alpha
Identification, Recovery, and Back-Up Procedures	.9462
Procedures for the DRP Plan, Human Resources, and Physical Facilities	.9499
Offsite Storage	.9291

As stated earlier, it is recommended that no matter which measure of internal consistency is used, an internal consistency reliability of .70 in the early stages of research, and a value above .80 or .90 in the advanced stages of research is considered satisfactory, while anything below .60 would indicate a lack of reliability (Nunnally & Bernstein, 1994). As can be seen from the tables above, except for perceived vulnerability which has a Cronbach's alpha of .6706, all the other scales demonstrate high reliabilities. And since the Cronbach's alpha for perceived vulnerability is also not

below the threshold value of .60 suggested by Nunnally and Bernstein (1994), it is concluded that it does not demonstrate a complete lack of reliability. The Cronbach's alphas for all the three newly formed dependent variables are very high thus adding support to conceptual reasoning behind their creation.

According to Diamantopoulos and Winklhofer (2001), elimination of items/indicators from formative constructs comes with the risk of altering the construct itself. Therefore, it does not seem appropriate to have an over all ITDRP construct when so many changes have been made in terms of removal of items and regrouping the retained items into new constructs. So instead of running a regression model with the independent variables and one dependent variable, the overall ITDRP, now it is more appropriate to run the regression with the independent variables on three separate dependent variables. Therefore, three separate regression models were formed as depicted in Figure 4.1, Figure 4.2, and Figure 4.3.

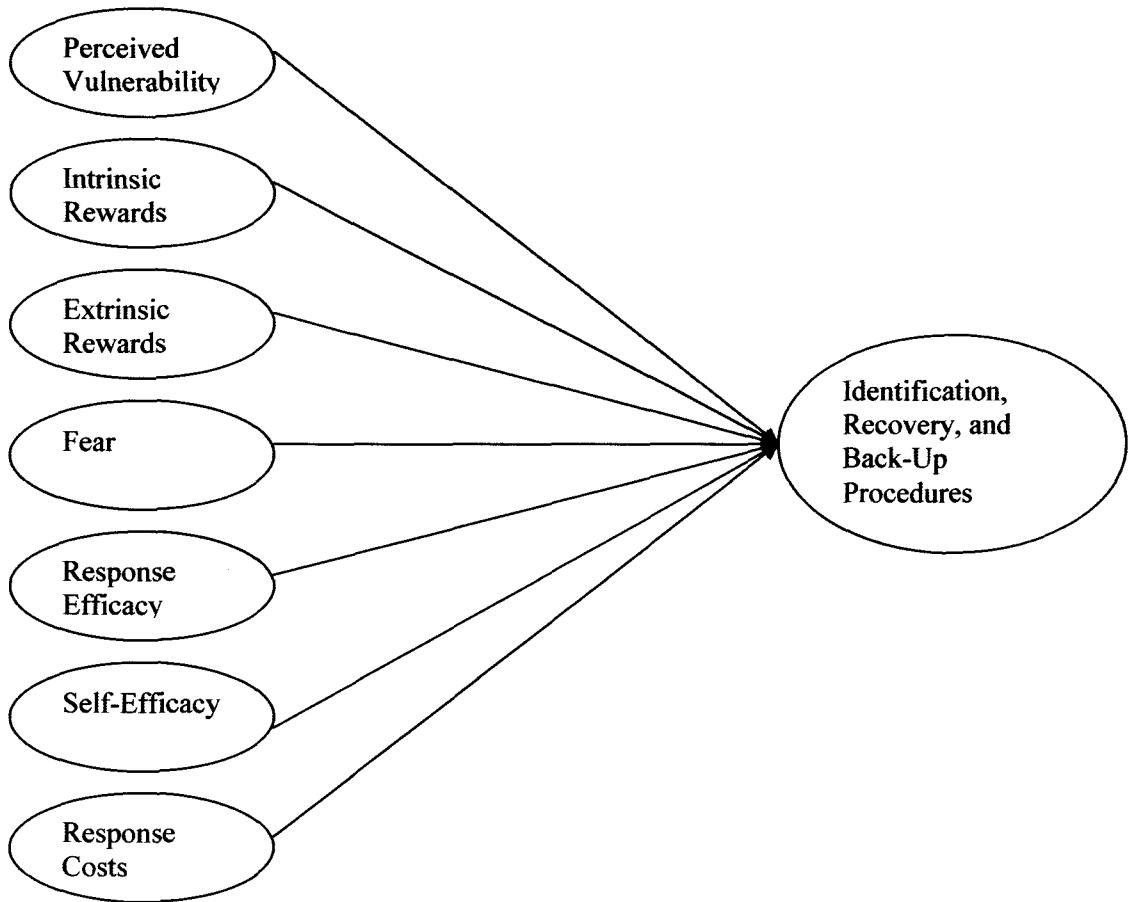


Figure 4.1. Regression Model 1

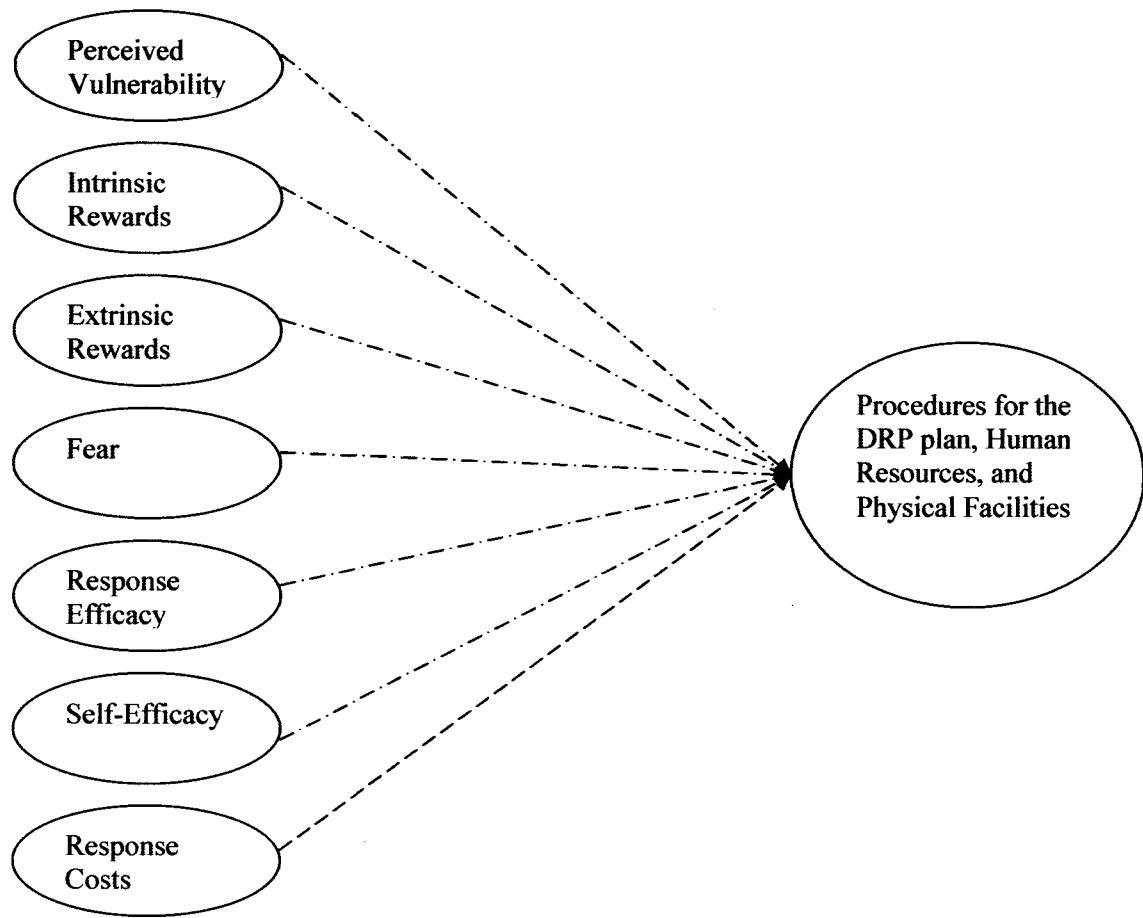


Figure 4.2. Regression Model 2

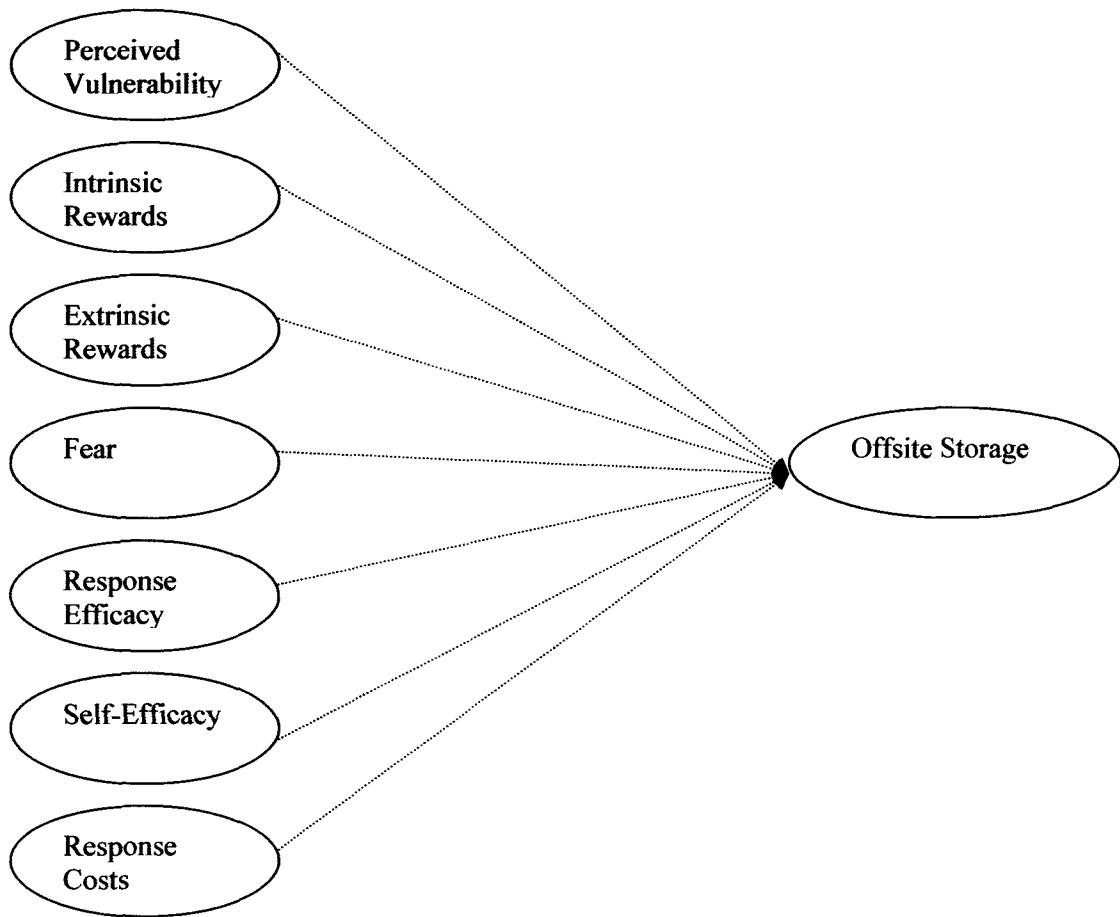


Figure 4.3. Regression Model 3

Checking Assumptions

Statistical procedures have underlying assumptions; in some cases the violations of these assumptions may not alter statistical research conclusions, but in some cases they might be critical (Garson, 2010). Kutner, Nachtsheim, Neter, and Li (2005) suggest that it is important to check the appropriateness of a model before any statistical inferences can be drawn. Therefore, the assumptions of linearity, normality, homogeneity of variance, outliers, influence, independence, multicollinearity, and fit of all the three regression models were checked. Except for a slight departure from normality for all the three

models and three outliers in Model 1, the rest of the assumptions were fully satisfied. This slight departure from normality raises the question of whether it warrants a data transformation or not. Although data transformation is recommended to remedy the presence of outliers and for departures from normality, linearity, and homoscedasticity, it is not universally recommended because transformed variables are more difficult to interpret (Tabachnick & Fidell, 2007). If the data is reasonably distributed with just a few outliers and having reasonably homogeneous variances, then there will not be much gained from the transformation. Therefore, the data is retained as it is for the analysis. There are only three significant outliers in Model 1 where the prediction is three standard deviations or more from the mean value of the dependent. There were no significant outliers found in Model 2 and Model 3. Since there are only few outliers, they can be dropped. But then, since this is the way the survey respondents chose to respond, deleting these outliers would mean throwing away data. Therefore, the outliers are retained, and since they are so few in number, data transformation has not been considered. The Brown and Forsythe test, which is a modification of the Levene test, does not depend on the normality of error terms and is considered to be robust test against departures from normality (Kutner et al., 2005). Therefore, the Brown-Forsythe test was conducted in order to check the homogeneity of variance assumption. The results were not significant at the .05 level of significance and therefore, the null hypothesis of equal variances cannot be rejected.

Leverage values greater than .50 or higher may be unduly influential and should be examined. Cook's distance of greater than one should be investigated for influence.

For all the three models, the leverage values are below .50 and all the Cook's distance values are below 1, therefore, influence is not a concern in any of the models.

The Durbin-Watson coefficient should be between 1.5 and 2.5 for independent observations. For Model 1, Model 2, and Model 3, the Durbin-Watson coefficient was 2.229, 2.074, and 1.864 respectively. Since the Durbin-Watson coefficient is below 2.5, independence assumption is satisfied in all the three models.

The variance inflation factor (VIF) was used to check the multicollinearity assumption. A threshold value of less than or equal to 3.3 has been recommended as being indicative of a lack of multicollinearity (Diamantopoulos and Siguaw 2006; Petter, Straub, and Rai 2007). All the VIFs were below the cut-off value of 3.3 and therefore, the assumption of no multicollinearity in all the models is satisfied.

The F test is recommended to determine whether a linear regression function is a good fit for the data or not (Kutner et al., 2005). The F test results indicated that all the three models were significant and linear. The F test value for all the three models are displayed in Table 4.6. Based on these results, it can be said that the model is significant and linear. The regression results for all the three models are presented in Table 4.6.

Table 4.6. Results of Multiple Regression Analysis

Variable	Hypothesis	Model 1	Model 2	Model 3
Perceived Vulnerability	1	-.031	.007	.081
Intrinsic Rewards	2	-.05	-.088	-.014
Extrinsic Rewards	3	.04	.000	-.068
Fear	4	-.01	.015	-.035
Response Efficacy	5	.01	-.04	.066
Self-Efficacy	6	.23**	.209**	.008
Response Costs	7	-.41***	-.385***	-.270**
F		9.696***	8.458***	4.272***
R ²		.278	.252	.145
Adjusted R ²		.250	.222	.111

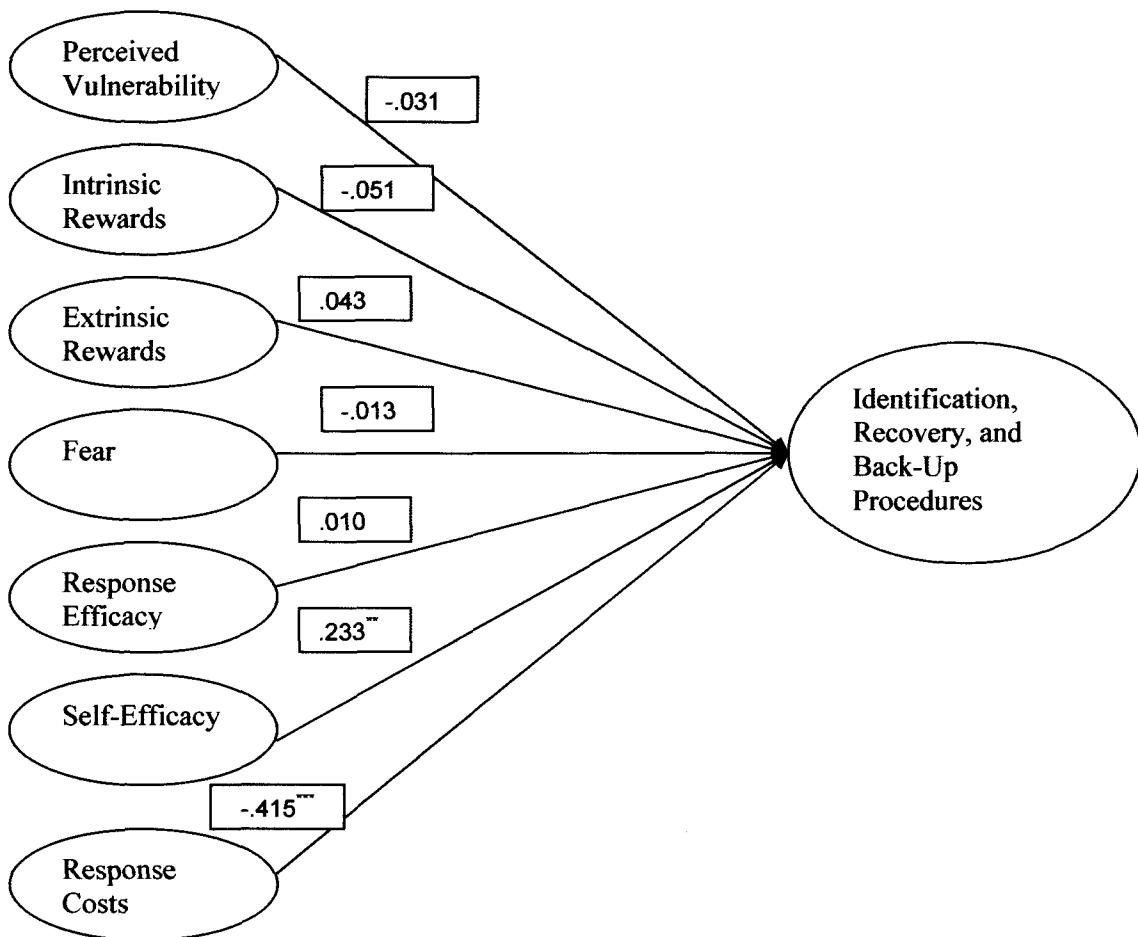
n = 184. Standard coefficients are shown.

*p value < 0.05; **p value < 0.01; ***p value < 0.001

The percent of the dependent variable explained by the independent variables is indicated by the R-square. For Model 1, 27.8% of the variance is explained by the model. For Model 2, 25.2% and for Model 3, 14.5% of variance is explained by the model. The adjustment to penalize for the possibility that with many independent variables some of the variance may be due to chance is indicated by the adjusted R-square. It implies that greater the number of independent variables, greater the adjustment penalty. Despite having seven independents in all the three models the penalty is minor. The F-statistic for all the three models is significant at p value < 0.001 indicating that the models are a good fit for the data.

Table 4.6 also shows the standardized beta coefficients and their associated significance levels. In Model 1, self-efficacy is significant at p value < 0.01, thus lending support to Hypothesis 6, which states that self-efficacy will have a significant positive

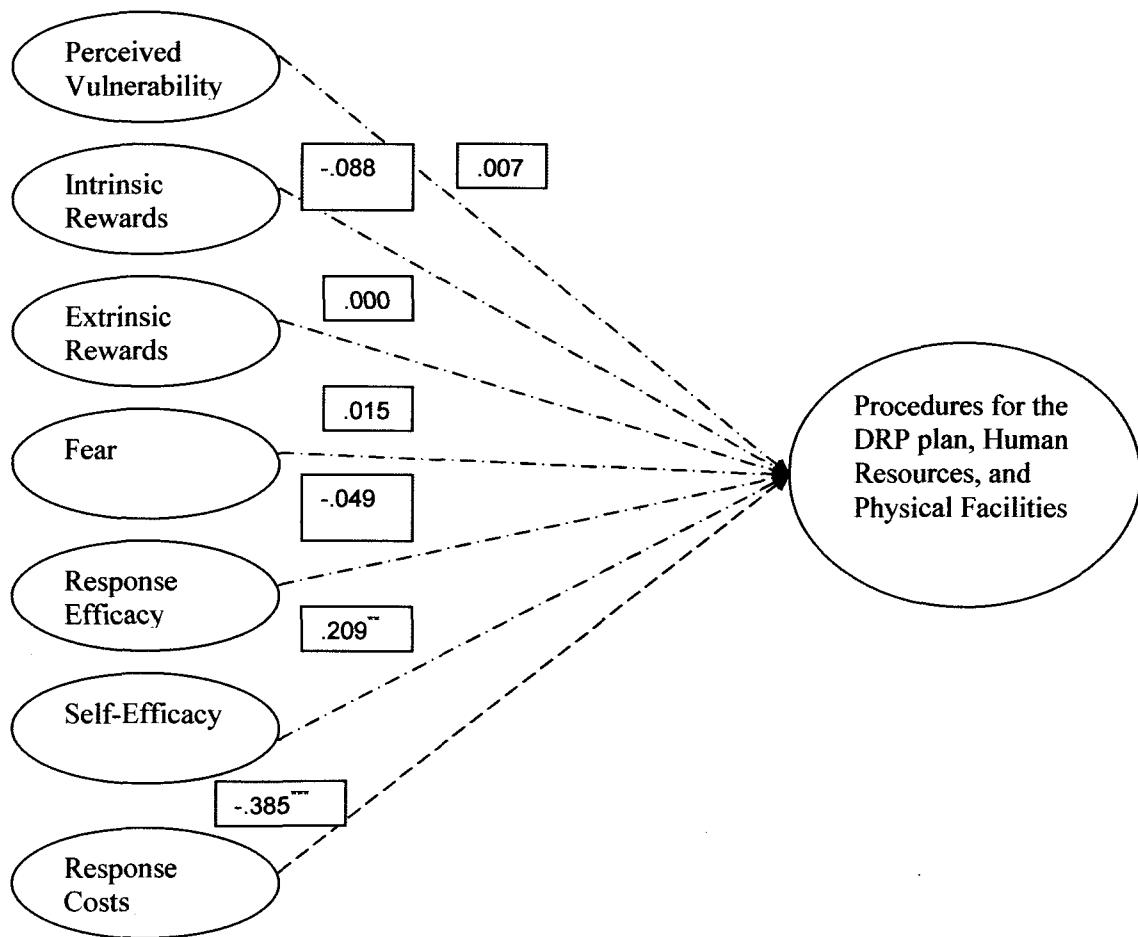
effect on an organization's identification, recovery, and back-up procedures. Response costs are also significant in Model 1 at p value < 0.001 and support Hypothesis 7, which states that response costs will have a significant negative effect on an organization's identification, recovery, and back-up procedures. Figure 4.4 displays the standardized beta coefficients for Model 1.



*p value < 0.05; **p value < 0.01; ***p value < 0.001

Figure 4.4. Model 1 Hypotheses

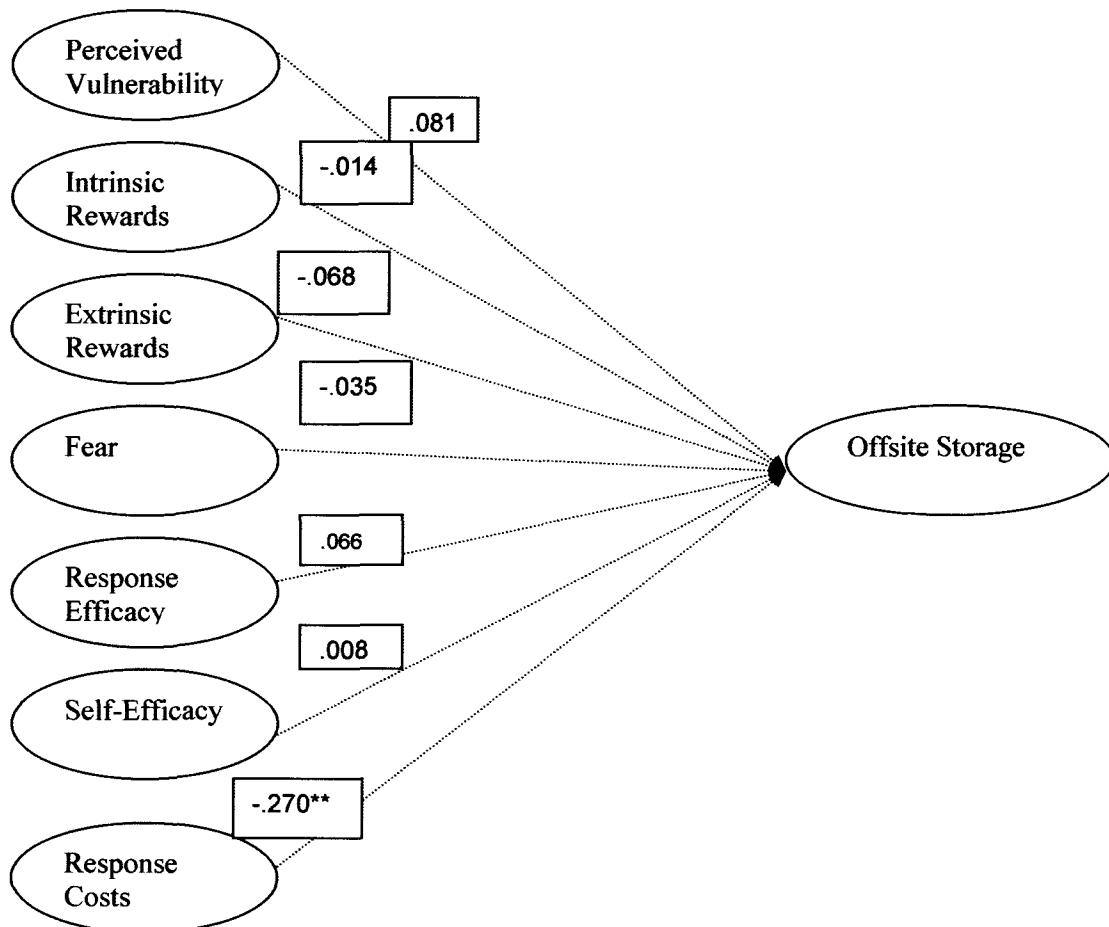
In Model 2, self-efficacy is significant at p value < 0.01, thus lending support to Hypothesis 6, which states that self-efficacy will have a significant positive effect on an organization's procedures for the DRP plan, human resources, and physical facilities. Response costs are also significant in Model 2 at p value < 0.001 and support Hypothesis 7, which states that response costs will have a significant negative effect on an organization's procedures for the DRP plan, human resources, and physical facilities. Figure 4.5 displays the standardized beta coefficients for Model 2.



*p value < 0.05; **p value < 0.01; ***p value < 0.001

Figure 4.5. Model 2 Hypotheses

In Model 3, only response costs are significant at p value < 0.01. This lends support to Hypothesis 7, which states that response costs will have a significant negative effect on an organization's offsite storage. Figure 4.6 displays the standardized beta coefficients for Model 3.



*p value < 0.05; **p value < 0.01; ***p value < 0.001

Figure 4.6. Model 3 Hypotheses

A summary of which hypotheses are supported and not supported in each of the three models is presented in Table 4.7.

Table 4.7. Hypotheses Supported/Not Supported

Model	Supported/Not Supported
Model 1	
H1: Perceived vulnerability will have a significant positive effect on an organization's identification, recovery, and back-up procedures.	Not Supported
H2: Intrinsic rewards will have a significant negative effect on an organization's identification, recovery, and back-up procedures.	Not Supported
H3: Extrinsic rewards will have a significant negative effect on an organization's identification, recovery, and back-up procedures.	Not Supported
H4: Fear will have a significant positive effect on an organization's identification, recovery, and back-up procedures.	Not Supported
H5: Response efficacy will have a significant positive effect on an organization's identification, recovery, and back-up procedures.	Not Supported
H6: Self-efficacy will have a significant positive effect on an organization's identification, recovery, and back-up procedures.	Supported
H7: Response costs will have a significant negative effect on an organization's identification, recovery, and back-up procedures.	Supported
Model 2	
H1: Perceived vulnerability will have a significant positive effect on an organization's procedures for the DRP plan, human resources, and physical facilities.	Not Supported
H2: Intrinsic rewards will have a significant negative effect on an organization's procedures for the DRP plan, human resources, and physical facilities.	Not Supported
H3: Extrinsic rewards will have a significant negative effect on an organization's procedures for the DRP plan, human resources, and physical facilities.	Not Supported
H4: Fear will have a significant positive effect on an organization's procedures for the DRP plan, human resources, and physical facilities.	Not Supported
H5: Response efficacy will have a significant positive effect on an organization's procedures for the DRP plan, human resources, and physical facilities.	Not Supported
H6: Self-efficacy will have a significant positive effect on an organization's procedures for the DRP plan, human resources, and physical facilities.	Supported

Table 4.7 (Continued)

H7: Response costs will have a significant negative effect on an organization's procedures for the DRP plan, human resources, and physical facilities.	Supported
Model 3	
H1: Perceived vulnerability will have a significant positive effect on an organization's offsite storage.	Not Supported
H2: Intrinsic rewards will have a significant negative effect on an organization's offsite storage.	Not Supported
H3: Extrinsic rewards will have a significant negative effect on an organization's offsite storage.	Not Supported
H4: Fear will have a significant positive effect on an organization's offsite storage.	Not Supported
H5: Response efficacy will have a significant positive effect on an organization's offsite storage.	Not Supported
H6: Self-efficacy will have a significant positive effect on an organization's offsite storage.	Not Supported
H7: Response costs will have a significant negative effect on an organization's offsite storage.	Supported

Based on the results, it is apparent that self-efficacy and response costs have been the significant driving forces in the research models of this study. A review of PMT research studies reveals that self-efficacy and response costs have proven to be significant driving forces of research models in various contexts. Posey (2010) also found more support for hypotheses derived from PMT's coping appraisal process than those derived from the threat appraisal process. Significant support was found for response costs in the study by Posey (2010). Both self-efficacy and response costs proved to be significant in the security compliance study of Herath and Rao (2009). Self-efficacy also has found support in the context of protective health behavior (Beck & Frankel, 1981), and in the context of security policy compliance (Siponen, Pahnila, & Mahmood, 2007). The results prove that even in an IT disaster recovery planning context, self-efficacy and response costs are significant factors.

It is interesting to note that although self-efficacy found support in the first two models dealing with procedures, it did not gain any support in the third model with offsite storage as the dependent variable. This implies that respondents feel that whether they have more offsite storage locations or not has nothing to do with their self-efficacy, but more to do with the response costs. However, all the procedural components of IT disaster recovery planning are driven not just by response costs, but by self-efficacy too as demonstrated by the support for self-efficacy in Models 1 and 2. On an intuitive level, it might be assumed that perceptions of threat, vulnerability, fear, and rewards might greatly influence IT disaster recovery planning. But the results of this study have shed light on the fact that for the success of IT disaster planning efforts it is important to ensure that employees have high levels of self-efficacy and believe that the response costs associated with such an endeavor wouldn't be high. In this way, the study offers practical insights to organizations and ITDRP professionals, while at the same time making a new and valuable contribution to the research literature.

CHAPTER 5

DISCUSSION AND CONCLUSION

In this chapter a brief summary of this dissertation will be presented, followed by a discussion of this study's contribution to the IS theory and implications for practice. The chapter ends with a discussion of the limitations of this study and possible future research directions.

Summary

Every year information losses caused by various disasters force many businesses to go out of operation temporarily or close down permanently. Yet the figures of staggering losses don't seem to be leading to preventive measures that can be steered by IT disaster recovery planning. Therefore, the purpose of this study was to investigate and find out what behavioral factors could be determining IT disaster recovery planning. To this end, protection motivation theory was applied as a theoretical lens. Protection motivation theory has been applied in various contexts, including IS literature, but has not specifically been applied in the disaster recovery planning context. IT disaster recovery planning construct with its sub-dimensions was developed by Shropshire and Kadlec (2009). So drawing from PMT literature and using the ITDRP construct developed by Shropshire and Kadlec (2009), a research model was developed in which

perceived severity, perceived vulnerability, intrinsic rewards, extrinsic rewards, fear, response efficacy, self-efficacy, and response costs are the determinants of ITDRP.

Most of the measures for the PMT constructs were drawn from existing scales and adapted to the IT disaster recovery planning context. Only items for intrinsic rewards and extrinsic rewards were developed in this study based on themes derived from Posey (2010). The measures for the ITDRP construct were taken as it is from Shropshire (2010).

Data was collected using Zoomerang's panel of IT disaster recovery planning professionals. 250 survey responses were collected. The data was examined closely to find patterns that revealed instances of respondents who had answered the survey without paying attention to the questions. After doing this, the sample size shrunk to only 184 usable responses. It was originally planned to use the PLS methodology to analyze the data, but given the small sample size and a large number of constructs and indicators, it was thought more appropriate to analyze the data using multiple regression analysis.

Principal components factor analysis was performed to ensure validity and Cronbach's alpha was used to assess scale reliability. Perceived severity and perceived vulnerability were loading on the same factor and a closer examination of the items revealed that there was some conceptual overlap and so it was decided to drop perceived severity from the model. The PCA of the ITDRP constructs revealed that items from the various ITDRP constructs were loading on three factors, thus warranting the creating of three new factors, namely: (1) identification, recovery, and back-up procedures; (2) procedures for the DRP plan, human resources, and physical facilities; and (3) offsite storage. This led to a revision of the research model. Three new regression models were formed with these three newly formed factors as the dependent variables and perceived

vulnerability, intrinsic rewards, extrinsic rewards, fear, response efficacy, self-efficacy, and response costs as the independent variables.

The regression results showed that self-efficacy and response costs were significant in Model 1 and 2, while only response costs was significant in Model 3. In most research studies that used PMT variables, self-efficacy and response costs were found to be significant variables in the research model. Therefore, the findings of this study add more support to self-efficacy and response costs as being significant drivers for protection motivated behaviors, in this context, IT disaster recovery planning. These findings also offer practical guidelines to organizations seeking to have successful IT disaster recovery planning and process.

Implications for IS Theory

As stated earlier, DRP although discussed in text books, has not received attention in mainstream IS research, which boasts of only 6 articles that were published in peer-reviewed MIS journals in the past ten years (Shropshire & Kadlec, 2009). There have been relatively few studies on pre-disaster planning efforts and IT-oriented disaster recovery planning research is scant (Shao, 2005). In such a scenario, this dissertation investigates IT disaster recovery planning through the lens of protection motivation theory, thus providing a theoretical framework. It examines from a behavioral perspective what could be the factors that influence IT disaster recovery planning.

This study developed measures for intrinsic rewards and extrinsic rewards in the IT disaster recovery planning context.

The ITDRP construct was recently developed by Shropshire and Kadlec (2009). Although, their study reported good scale validity and reliability for all the scales, a

principal components analysis (PCA) revealed that items from several different constructs were loading on the same component. Based on a closer examination of the individual items and the loadings, two of the ITDRP constructs, namely, preparing organizational members and IT service analysis were removed from the model and the remaining items were reorganized to form three new constructs. These three new ITDRP constructs are as follows: (1) identification, recovery, and back-up procedures; (2) procedures for the DRP plan, human resources, and physical facilities; and (3) offsite storage.

Although, it might generally be assumed that financial costs, threat, vulnerability, rewards, and fear might be the driving forces for IT disaster recovery planning. The findings of this study, however tell a different story. Self-efficacy and response costs were found to be the only significant factors in the model. Therefore, this dissertation contributes to the body of literature on IT disaster recovery planning by applying a theoretical framework and bringing in a new perspective.

Implications for IS Practice

Despite the losses suffered due to loss of information and systems due to various disasters, IT disaster recovery planning is not always undertaken by organizations and even when it is undertaken, it is riddled with problems. In a study of companies that suffered a major data loss and did not have a BC/DR plan, 43% never reopen, 51% close within two years, and only 6% survive in the long run (Cummings, Haag, & McCubrey, 2005; Snedaker, 2007). Mitroff, Harrington, and Gai (1996) state that organizations that prepare for crisis, usually recover three times faster than the unprepared organizations, and also face significantly less financial and human cost. Yet, the Info-Tech Research

Group reports that 60% of North American businesses do not have a DR plan (Chisholm, 2008). This raises a question as to what are the factors that influence disaster recovery planning. And this study tries to answer it using a theoretical lens. The results shed light on the fact that for the success of IT disaster planning efforts it is important to ensure that employees have high levels of self-efficacy and believe that the response costs associated with such an endeavor wouldn't be high. In this way, the study offers practical insights to organizations and ITDRP professionals, while at the same time making a new and valuable contribution to the research literature. Self-efficacy was found to be significantly related to both the procedures oriented factors. This indicates that if it is felt that the IT disaster recovery planning is complicated or has many procedures, then it can become daunting and discourage people from undertaking and implementing IT disaster recovery planning. Therefore, organizations seeking to implement IT disaster recovery planning should be cognizant of this fact and take care to ensure that the IT disaster recovery planning and procedures don't appear to be too cumbersome.

This dissertation sheds light on the behavioral dynamics of the IT disaster recovery planning process from a protection motivation perspective; understanding which might be a key in the successful implementation of IT disaster recovery plans and saving of time and other resources and guard against the possibility of failed or abandoned DRP projects.

Limitations and Future Research

The sample size of only 184 might limit greater over all generalizability. The original model and the revised models should be tested by collecting more data. And PLS might be used if the sample size is larger.

Perceived severity was removed from the original model as it was loading on the same factor as perceived vulnerability and there was some conceptual overlap in the items. Additionally, the scale for perceived vulnerability has a reliability of only .60. Therefore, indicating that the items of both these constructs should be reanalyzed and new items leading to higher scale reliabilities and better validity should be developed or adapted.

Other factors such as organizational leadership, organizational structure, and opinion leadership might have a moderating effect. Moreover, influence of factors such as organizational size and annual revenue might also be examined. These are some of the directions that future research can take, thus building on the frameworks and findings presented in this dissertation.

APPENDIX A

SURVEY INSTRUMENT



SURVEY - Information Technology Disaster Recovery Planning

Created: August 24 2010, 3:14 PM
 Last Modified: October 11 2010, 12:44 PM
 Design Theme: Basic Blue
 Language: English
 Button Options: Labels
 Disable Browser "Back" Button: False

SURVEY - Information Technology Disaster Recovery Planning

Page 1 - Heading

Page 1 of 8

Page 1 - Question 1 - Choice - One Answer (Bullets)

[Mandatory]

I have read and understood the description of the study, and its purposes and methods. I am an Information Technology Professional involved in Disaster Recovery Planning, and therefore I meet the requirement to participate in this study. I understand that my participation in this research is completely voluntary and my participation or refusal to participate in this study will not affect my relationship with my employer or with Louisiana Tech University. I understand that my anonymity is fully ensured.

- Yes, I accept
- No, I decline [Screen Out]

Page 2 - Heading

Page 2 of 8

Page 2 - Heading

Please evaluate each of the following items indicating your agreement or disagreement with each statement.

Page 2 - Question 2 - Rating Scale - Matrix

[Mandatory] [Randomize]

Perceived Severity

	strongly disagree	moderate ly disagree	slightly disagree	neither agree nor disagree	slightly agree	moderate ly agree	strongly agree
If our organization were to face a disaster, we would lose information and systems.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Facing disaster would be unlikely to cause any loss of data and systems for our organization.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I believe that the threat of disaster to our organization is severe.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I believe that the threat of disaster to our organization is slight.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Page 2 - Question 3 - Rating Scale - Matrix

[Mandatory] [Randomize]

Perceived Vulnerability

strongly	moderate	slightly	neither	slightly	moderate	strongly
----------	----------	----------	---------	----------	----------	----------

planning will save a lot of time. Disaster recovery planning is time consuming, so skipping disaster recovery planning steps will save time. Disaster recovery planning guidelines are too restrictive and limit work efficiency.

Page 3 - Heading
Page 3 of 8

Disaster recovery planning is an effective method to prevent loss and damage to information systems due to a disaster.

○ ○ ○ ○ ○ ○ ○

If we undertake the recommended disaster recover planning, we are less likely to face any loss or damage due to disaster.

○ ○ ○ ○ ○ ○ ○

Page 3 - Question 8 - Rating Scale - Matrix

[Mandatory] [Randomize]

Page 3 - Question 9 - Rating Scale - Matrix

[Mandatory] [Randomize]

exercises as we would feel silly doing so.

Page 4 - Heading
Page 4 of 8

Page 4 - Question 10 - Rating Scale - Matrix [Mandatory] [Randomize]

Please evaluate each of the following items indicating your agreement or disagreement with each statement.

We have established an alternative means of communications (e.g. cell phones) to use in emergencies.

Page 6 - Question 15 - Rating Scale - Matrix [Mandatory] [Randomize]

Page 6 - Question 16 - Rating Scale - Matrix [Mandatory] [Randomize]
Information Technology Services Analysis

Page 6 - Question 17 - Rating Scale - Matrix [Mandatory] [Randomize]

configuration files, change logs, and other relevant documents.

We have offsite locations for storing copies of the information technology disaster recovery plan.

Page 7 - Question 20 - Rating Scale - Matrix [Mandatory]

Maintenance

	strongly disagree	moderately disagree	slightly disagree	neither agree nor disagree	slightly agree	moderately agree	strongly agree
We have procedures for testing of the information technology disaster recovery plan.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
We have procedures for updating the information technology disaster recovery plan.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
We have procedures for ensuring that the information technology disaster recovery plan is part of the business continuity plan.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
We have procedures for documenting system configurations, changes, and updates.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Page 8 - Heading

Page 8 of 8

Page 8 - Heading

Demographics etc.

For the following questions, please select the appropriate answer.

Page 8 - Question 21 - Choice - One Answer (Bullets)

[Mandatory]

What is your gender?

- Male
- Female

Page 8 - Question 22 - Choice - One Answer (Bullets)

[Mandatory]

What is your age?

- less than 21 yrs
- 21-25 yrs
- 26-35 yrs
- 36-45 yrs
- 46-55 yrs
- over 55 yrs

Page 8 - Question 23 - Choice - One Answer (Bullets)

[Mandatory]

What is your highest level of education?

- High school
- Bachelor's
- Master's
- Professional
- Doctorate

Page 8 - Question 24 - Choice - One Answer (Bullets)

[Mandatory]

Organizational Size

Number of full-time employees in your organization:

- 1-100
- 101-500
- 501-1,000
- 1,001-5,000
- more than 5,000

Page 8 - Question 25 - Choice - One Answer (Bullets)

[Mandatory]

How long have you been working in this organization?

- Less than 1 yr
- 1-5 yrs
- 6-10 yrs
- 11-15 yrs
- 16-20 yrs
- 21 yrs or more

Page 8 - Question 26 - Choice - One Answer (Bullets)

[Mandatory]

For how long have you been involved in activities related to "Disaster Recovery Planning" in your current organization?

- Less than 1 yr
- 1-5 yrs
- 6-10 yrs
- 11-15 yrs
- 16-20 yrs
- 21 yrs or more

Page 8 - Question 27 - Choice - One Answer (Bullets)

[Mandatory]

Your job role relates to

- Information Technology
- Other

Page 8 - Question 28 - Choice - One Answer (Bullets)

[Mandatory]

Your organization works in which industry?

- Manufacturing
- Retail
- Services

- Entertainment
- Education
- Voluntary not for profit
- Other

Page 8 - Question 29 - Choice - One Answer (Bullets)

[Mandatory]

Your company is organized as a

- Publicly Traded Corporation
- Privately Held Corporation
- Non-profit Corporation
- Limited Liability Company (LLC)
- Partnership
- Other

Page 8 - Question 30 - Choice - One Answer (Bullets)

[Mandatory]

The annual revenue of your company is

- Less than \$ 1 million
- \$1 million - \$10 million
- \$11 million - \$100 million
- \$101 million - \$1 billion
- more than \$1 billion

Thank You Page

Screen Out Page

Over Quota Page

Survey Closed Page

(Standard - Zoomerang branding)

APPENDIX B

HUMAN USE LETTER



LOUISIANA TECH
U N I V E R S I T Y
MEMORANDUM

OFFICE OF UNIVERSITY RESEARCH

TO: Ms. Shalini Wunnava, Dr. Tom Roberts and Dr. Selwyn Ellis
 FROM: Barbara Talbot, University Research
 SUBJECT: HUMAN USE COMMITTEE REVIEW
 DATE: June 24, 2010

In order to facilitate your project, an EXPEDITED REVIEW has been done for your proposed study entitled:

**"Application of Protection Motivation Theory to
 Disaster Recovery Planning: An Empirical Investigation"**

HUC-775

The proposed study's revised procedures were found to provide reasonable and adequate safeguards against possible risks involving human subjects. The information to be collected may be personal in nature or implication. Therefore, diligent care needs to be taken to protect the privacy of the participants and to assure that the data are kept confidential. Informed consent is a critical part of the research process. The subjects must be informed that their participation is voluntary. It is important that consent materials be presented in a language understandable to every participant. If you have participants in your study whose first language is not English, be sure that informed consent materials are adequately explained or translated. Since your reviewed project appears to do no damage to the participants, the Human Use Committee grants approval of the involvement of human subjects as outlined.

Projects should be renewed annually. *This approval was finalized on June 24, 2010 and this project will need to receive a continuation review by the IRB if the project, including data analysis, continues beyond June 24, 2011.* Any discrepancies in procedure or changes that have been made including approved changes should be noted in the review application. Projects involving NIH funds require annual education training to be documented. For more information regarding this, contact the Office of University Research.

You are requested to maintain written records of your procedures, data collected, and subjects involved. These records will need to be available upon request during the conduct of the study and retained by the university for three years after the conclusion of the study. If changes occur in recruiting of subjects, informed consent process or in your research protocol, or if unanticipated problems should arise it is the Researchers responsibility to notify the Office of Research or IRB in writing. The project should be discontinued until modifications can be reviewed and approved.

If you have any questions, please contact Dr. Mary Livingston at 257-4315.

A MEMBER OF THE UNIVERSITY OF LOUISIANA SYSTEM

P.O. BOX 3092 • RUSTON, LA 71272 • TELEPHONE (318) 257-5075 • FAX (318) 257-5079
 AN EQUAL OPPORTUNITY UNIVERSITY

REFERENCES

- Adam, F. and J. A. Haslam. 2001. The Irish experience with disaster recovery planning: High levels of awareness may not suffice. In *Information security management: global challenges in the new millennium*. New York, NY: Idea Group Publishing.
- Allison, D. H. and P. B. Deblois. 2008. Top 10 IT issues. *EDUCAUSE* May/June: 37-61.
- Anderson, J. 2008. New trends in backup: Is your disaster recovery plan keeping up? *The eSecurity Advisor* 8 (2): 58.
- Anonymous. 2003. Survey reveals disaster recovery expectations and reality. *Information Management Journal* 37 (6): 8.
- Bandura, A. 1982. Self-efficacy mechanism in human agency. *American Psychologist* 37 (2): 122-147.
- Bagozzi, R. P. 1994. Structural equation models in marketing research: Basic principles. In *Principle of marketing research*. 317-85. Oxford: Blackwell.
- Beck, K. H. and A. Frankel. 1981. A conceptualization of threat communications and protective health behavior. *Social Psychology Quarterly* 44 (3): 204-217.
- Block, L. G. and P. A. Keller. 1995. When to accentuate the negative: The effects of perceived efficacy and message framing intentions to perform a health-related behavior. *Journal of Marketing Research* 32 (2): 192-203.
- Bolch, M. 2008. Creating a disaster recovery plan is just the first step.
http://searchdisasterrecovery.techtarget.com/news/article/0,289142,sid190_gci133_0327,00.html (accessed December 6, 2009).
- Brouwers, M. C. and R. M. Sorrentino. 1993. Uncertainty orientation and protection motivation theory: The role of individual differences in health compliance. *Journal of Personality and Social Psychology* 65 (1): 102-112.
- Brunetto, G. and N. L. Harris. 2001. Disaster recovery: How will your company survive? *Strategic Finance* 82 (9): 57-61.

- Buchanan, Robert W. 2003. *Disaster proofing information systems: a complete methodology for eliminating single points of failure*. New York: McGraw-Hill.
- Chin, W. W. 1998. Issues and opinion on structural equation modeling. *MISQ* 22 (1).
- Chisholm, P. 2008. Disaster recovery planning is business-critical. *The CPA Journal* 78 (7): 11.
- Churchill, G. A., Jr. 1979. A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research* 16 (1): 64-73.
- Churchill, Jr., Gilbert A. and Dawn Iacobucci 2002. *Marketing research: methodological foundations*. Fort Worth: Harcourt Dryden.
- Cismaru, M. and A. M. Lavack. 2007. Interaction effects and combinatorial rules governing protection motivation theory: A new model. *Marketing Theory* 7 (3): 249-270.
- Cole, Eric, Ronald. L. Krutz, and J. Conley. 2005. *Network security bible*. New York: John Wiley & Sons, Inc.
- Cummings, M., S. Haag, and D. J. McCubrey. 2005. *Management information systems for the information age*. New York: McGraw-Hill Ryerson Higher Education.
- Diamantopoulos, A. and H. M. Winklhofer. 2001. Index construction with formative indicators: An alternative to scale development. *Journal of Marketing Research* 38 (2): 259-277.
- Diamantopoulos, A., and J. A. Siguaw. 2006. Formative versus reflective indicators in organizational measure development: A comparison and empirical illustration. *British Journal of Management* 17 (4): 263-282.
- Eppright, D. R., J. B. Hunt., J. F. Tanner, Jr., and G. R. Franke. 2002. Fear, coping, and information: A pilot study on motivating a healthy response. *Health Marketing Quarterly* 20 (1): 51-73.
- Fallara, P. 2003. Disaster recovery planning: The best defense is a well managed offense. *IEEE Potentials* 22 (5): 40-44.
- Farazmand, A. 2007. Learning from the Katrina crisis: A global and international perspective with implications for future crisis management. *Public Administration Review* 67 (1): 149-159.
- Floyd, D. L., S. Prentice-Dunn., and R. W. Rogers. 2000. A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology* 30 (2): 407-429.

- Garson, G. D. 2010. Testing of assumptions, from *Statnotes: Topics in multivariate analysis*. <http://faculty.chass.ncsu.edu/garson/pa765/statnote.htm> (accessed December 4, 2010).
- Gatlin, H. N. 2006. *The search for a theoretical framework for long-term disaster recovery efforts: a normative application of Jane Addams' social democratic theory and ethics*. San Marcos, Texas: Texas State University. <http://ecommons.txstate.edu/arp/125> (accessed June 30, 2009).
- Gefen, D., D. W. Straub., and M. Boudreau. 2000. Structural equation modeling and regression: guidelines for research practice. *Communications of the Association for Information systems* 4 (7): 1-77.
- Gollwitzer, P. M. 1993. Goal achievement: The role of intentions. In *Stroebe, W. and M. Hewstone, eds., European review of social psychology* 4: 141-185. Chichester: Wiley.
- Hair, J. F., Jr., R. E. Anderson, R. L. Tatham, and W. C. Black. 1998. *Multivariate data analysis with readings*. Englewood Cliffs, NJ: Prentice Hall.
- Heckhausen, H. 1991. *Motivation and action*. Berlin & New York: Spring-Verlag.
- Herath, T. and H. R. Rao. 2009. Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems* 18 (4): 1-20.
- Herzog, R.J. 2007. A model of natural disaster administration: Naming and framing theory and reality. *Administrative Theory & Praxis* 29 (4): 586-604.
- Hoffer, J. 2001. Backing up business: Industry trend or event. *Health Management Technology*. http://findarticles.com/p/articles/mi_m0DUD/is_1_22/ai_68864006.htm (accessed January 16, 2008).
- Hovland, C. I., I. L. Janis, and J. J. Kelley. 1953. *Communication and persuasion*. New Haven: Yale University Press.
- Jackson, R. 2008. In times of crisis. *Internal Auditor* 31 (4): 46-51.
- Kerlinger, F. and H. B. Lee. 2000. *Foundations of behavioral research*. Orlando: Harcourt.
- Kutner, M. H., C. J. Nachtsheim, J. Neter, and W. Li. 2005. *Applied linear statistical models*. Singapore: McGraw-Hill.

- Luftman, J., and R. Kempaiah. 2007. Key issues for IT executives 2007. *MIS Quarterly Executive* 7 (2): 99-112.
- Maddux, J. E., and R. W. Rogers. 1983. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology* 19 (September): 469-479.
- McClain, J., J. M. Bernhardt, and M. J. Beach. 2005. Assessing parents' perception of children's risk for recreational water illnesses. *Emerging Infectious Diseases* 11 (5): 670-676.
- Milne, S., P. Sheeran, and S. Orbell. 2000. Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology* 30: 106-143.
- Milne, S., S. Orbell., and P. Sheeran. 2002. Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. *British Journal of Health Psychology* 7: 163-184.
- Mitroff, I. I., L. K. Harrington, and E. Gai. 1996. Thinking about the unthinkable. *Across the Board* 33 (8): 44-48.
- Norman, P., H. Boer, and E. R. Seydel. 2005. Protection motivation theory. In *Predicting health behavior*, Conner, M., and P. Norman, eds. 170-222. Berkshire: Open University Press.
- Nunnally, J. C., and I. H. Bernstein. 1994. *Psychometric theory*. 3rd eds. New York, NY: McGraw-Hill.
- Pechmann, C., G. Zhao, M. E. Goldberg, and E. T. Reibling. 2007. What to convey in antismoking advertisements for adolescents: The use of protection motivation theory to identify effective message themes. *Journal of Marketing* 67 (4): 1-18.
- Pedhazur, E. J. and L. P. Schmelkin. 1991. *Measurement, design, and analysis: An integrated approach*. Hillsdale: Lawrence Erlbaum Associates.
- Petter, S., D. Straub., and A. Rai. 2007. Specifying formative constructs in information systems research. *MIS Quarterly* 31 (4): 623-656.
- Piotrowski, C. 2006. Hurricane Katrina and organization development: Part 1 – Implications of chaos theory. *Organization Development Journal* 24 (3): 10-19.
- Posey, M. C. 2010. Protection-motivated behaviors of organizational insiders. DBA dissertation. *Louisiana Tech University*.
- Preimesberger, C. 2008. On the brink of disaster. *eWeek* 11 (2): 31-38.

- Prentice-Dunn, S., and R. W. Rogers. 1986. Protection motivation theory and preventive health: Beyond the health belief model. *Health Education Research* 1 (3): 153-161.
- Rennels, B. 2006. Disaster recovery planning: A practical guide to starting the plan introduction. <http://www.doubletake.com> (accessed December 18, 2007).
- Rippetoe, P. A. and R. W. Rogers. 1987. Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology* 52 (10): 596-604.
- Rogers, R. W. 1975. A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91 (4): 93-114.
- Rogers, R. W. 1983. Cognitive and physiological process in fear appeals and attitude change: A revised theory of protection motivation. 153-174. In *social psychophysiology*. J. Cacioppo and R. Petty, Eds., New York: The Guilford Press.
- Shao, B. B. M. 2005. Optimal redundancy allocation for information technology disaster recovery in the network economy. *IEEE Transactions on Dependable and Secure Computing* 2 (3): 262-267.
- Shropshire, J. and C. Kadlec. 2009. Developing the IT disaster recovery planning construct. *Journal of Information Technology Management*, XX (4): 37-56.
- Siponen, M., S. Pahnila, and A. Mahmood. 2007. Employees' adherence to information security policies: An empirical study. In *new approaches for security, privacy and trust in complex environments*, edited by H. Venter, M. Eloff, L. Labuschagne, J. Eloff and R. Von Solms. Boston: Springer.
- Snedaker, S. 2007. *Business continuity & disaster recovery for IT professionals*. Burlington: Syngress Publishing, Inc.
- Straub, D. 1989. Validating instruments in MIS research. *MIS Quarterly* 13 (2): 147-169.
- Sturges, J. and R. W. Rogers 1996. Preventive health psychology from a developmental perspective: An extension of protection motivation theory. *Health Psychology* 15 (3): 158-166.
- Tabachnick, B. G., and Fidell, L. S. 2007. *Using multivariate statistics* (5th ed.). Boston: Allynand Bacon.
- Tanner, Jr. J. F., E. Day, and M. R. Crask. 1989. Protection motivation theory: An extension of fear appeals theory in communications. *Journal of Business Research* 19 (4): 267-76.

- Tanner, Jr. J. F., J. B. Hunt, and D. R. Eppright. 1991. The protection motivation model: A normative model of fear appeals *Journal of Marketing* 55 (3): 36-45.
- Taylor, A. H. and S. May. 1996. Threat and coping appraisal as determinants of compliance with sports injury rehabilitation: An application of protection motivation theory *Journal of Sports Sciences* 14 (9): 471-482.
- Toigo, Jon W. 2000. *Disaster recovery planning*. New York: Prentice Hall.
- Veritas Disaster Recovery Research Seminar 2004. Protect your network. Why disaster recovery is important.
http://download.microsoft.com/download/9/D/5/9D535435-954D-47F6-92B5-5125B1291EB7/May_25_SB_MS%20Security%20Seminar%20250505.ppt
(accessed December 2, 2009).
- Whetten, D. A. 1989. What constitutes a theoretical contribution? *Academy of Management Review* 14 (4), 490-495.
- Whitman, M. E. and H. J. Mattord 2007. *Principles of information security*. Course Technology.
- Witte, K. 1992. The role of threat and efficacy in AIDS prevention. *International Quarterly of Community Health Education* 12 (8): 225-249.
- Witte, K., K. A. Cameron, J. McKeon, and J. Berkowitz. 1996. Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of Health Communication*. 1 (5): 317-341.
- Workman, M., W. Bommer, and D. Straub. 2008. Security lapses and the omission of information security measures: An empirical test of the threat control model. *Journal of Computers in Human Behavior* 24 (4): 2799-2816.